NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

A THEORY OF DARK NETWORK DESIGN

by

Ian S. Davis
Carrie L. Worth
Douglas W. Zimmerman

December 2010

Thesis Advisor:	Nancy Roberts
Second Reader:	John Arquilla

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE *Form Approved OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2010	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE A Theory of Dark Network Design

5. FUNDING NUMBERS

6. AUTHOR(S) Ian S. Davis, Carrie L. Worth, Douglas W. Zimmerman

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number _____N/A_____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

This study presents a theory of dark network design and answers two fundamental questions about illuminating and interdicting dark networks: how are they configured and how are they vulnerable? We define dark networks as interdependent entities that use formal and informal ties to conduct licit or illicit activities and employ operational security measures and/or clandestine tradecraft techniques through varying degrees of overt, or more likely covert, activity to achieve their purpose. A dark network must design itself to buffer environmental hostility and produce output to achieve its purpose according to its design state. The level of hostility in the environment and the requirement for secure coordination of work determine the dark network's design state. These factors yield four typological dark network configurations: Opportunistic-Mechanical; Restrictive-Organic; Selective-Technical; and Surgical-Ad hoc. Each configuration must allow the secure coordination of work between the dark network's directional, operational, and supportive components and should adhere to the six principles of dark network design we identify: security, agility, resilience, direction setting, control, and capacity. If a dark network's configuration does not fit its design state or violates the principles of dark network design, the network will be vulnerable to illumination and interdiction.

14. SUBJECT TERMS
Dark Network Theory, Network Design, Clandestine Networks, Covert Action, Network Warfare, Network Configuration, Network Vulnerability, Disruption, Systems Model, Network Analysis, Mara Salvatrucha-13, Provisional Irish Republican Army, Hezbollah, Hamburg, al-Qa'ida

15. NUMBER OF PAGES
177

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

THE THEORY OF DARK NETWORK DESIGN

Ian S. Davis
Major, United States Army
B.S., Regents College, 1999

Carrie L. Worth
Major, United States Air Force
B.S., United States Air Force Academy, 1997
M.S., Embry-Riddle Aeronautical University, 2007

Douglas W. Zimmerman
Major, United States Army
B.S., University of Iowa, 1993

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN DEFENSE ANALYSIS

from the

NAVAL POSTGRADUATE SCHOOL
December 2010

Authors: Ian S. Davis
Carrie L. Worth
Douglas W. Zimmerman

Approved by: Dr. Nancy Roberts
Thesis Advisor

Dr. John Arquilla
Second Reader

Dr. Gordon H. McCormick
Chairman, Department of Defense Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This study presents a theory of dark network design and answers two fundamental questions about illuminating and interdicting dark networks: how are they configured and how are they vulnerable? We define dark networks as interdependent entities that use formal and informal ties to conduct licit or illicit activities and employ operational security measures and/or clandestine tradecraft techniques through varying degrees of overt, or more likely covert, activity to achieve their purpose. A dark network must design itself to buffer environmental hostility and produce output to achieve its purpose according to its design state. The level of hostility in the environment and the requirement for secure coordination of work determine the dark network's design state. These factors yield four typological dark network configurations: Opportunistic-Mechanical; Restrictive-Organic; Selective-Technical; and Surgical-Ad hoc. Each configuration must allow the secure coordination of work between the dark network's directional, operational, and supportive components and should adhere to the six principles of dark network design we identify: security, agility, resilience, direction setting, control, and capacity. If a dark network's configuration does not fit its design state or violates the principles of dark network design, the network will be vulnerable to illumination and interdiction.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION 1
- A. PURPOSE AND SCOPE 1
- B. APPLICABILITY 2
- C. THE NATURE OF DARK AND LIGHT NETWORKS 5
  - 1. Definitions 5
  - 2. Dimensions to Compare and Contrast Networks 8
    - *a. Hostility of the Environment 8*
    - *b. Secure Coordination of Work 9*
  - 3. Network Types 9
    - *a. Dark Networks 10*
    - *b. Light/Bright Networks 10*
    - *c. Gray Networks 10*
- D. IMPACT OF THE STUDY 12
- E. THESIS ORGANIZATION 13

II. LITERATURE REVIEW 15
- A. INTRODUCTION 15
- B. ORGANIZATION DESIGN 15
  - 1. External Dimension: The Environment 19
    - *a. The Simple-Complex Dimension 20*
    - *b. The Stable-Unstable Dimension 21*
    - *c. The Environment and Uncertainty 21*
  - 2. Internal Dimension: Configuration 24
    - *a. Configuration 24*
    - *b. Mintzberg's Organizational Configurations 24*
    - *c. Components of Configurations 27*
    - *d. Design Elements of Configurations 27*
    - *e. Summary of Configuration 28*
- C. NETWORK LITERATURE 29
  - 1. Basic Features of Networks 30
    - *a. Network Assets 31*
    - *b. Network Facets 31*
    - *c. Network Relationships 32*
    - *d. Network Structures 35*
    - *e. Network Governance 36*
    - *f. Network Design 38*
  - 2. Dark Networks 39
    - *a. External Dimension: Hostility of the Environment ... 40*
    - *b. Internal Dimension: Secure Coordination of Work .. 42*
- D. SHORTFALLS IN THE LITERATURE 50
- E. CONCLUSION 52

III. THEORY OF DARK NETWORK DESIGN 53

A. INTRODUCTION 53
B. DIMENSIONS OF DARK NETWORK DESIGN 54
1. External Dimension: Hostility of the Environment 54
2. Internal Dimension: Secure Coordination of Work............. 54
C. DARK NETWORK TYPOLOGY.. 54
1. Type I: Opportunistic-Mechanical 55
2. Type II: Restrictive-Organic 55
3. Type III: Selective-Technical.. 56
4. Type IV: Surgical-Ad Hoc 56
D. DARK NETWORK COMPONENTS... 57
1. Directional Component 57
a. Core Directors 57
b. Peripheral Directors.. 58
2. Operational Component... 58
a. Lethal Action 58
b. Non-Lethal Action 59
3. Supportive Component 59
a. Active Support 59
b. Passive Support... 60
E. CHALLENGES AND PRINCIPLES OF DARK NETWORK DESIGN... 61
1. Buffering External Hostility.. 61
2. Coordinating Work to Produce Output 62
F. DARK NETWORK SYSTEM MODEL 63
G. CONCLUSION 63

IV. TYPE-I DARK NETWORK: OPPORTUNISTIC-MECHANICAL 65
A. INTRODUCTION... 65
B. OVERVIEW OF MARA SALVATRUCHA-13 66
C. TYPE-I DESIGN STATE 69
1. Moderate Hostility of the Environment 69
2. Moderate Requirement for Secure Coordination of Work.. 70
D. TYPE-I DARK NETWORK: OPPORTUNISTIC-MECHANICAL 70
1. Opportunistic Action 70
2. Mechanical Configuration.. 71
E. FUNDAMENTAL COMPONENTS 73
1. Directional Component 74
2. Operational Component... 77
3. Supportive Component 79
F. VULNERABILITIES AND CONCLUSION... 82

V. TYPE-II DARK NETWORK: RESTRICTIVE-ORGANIC................................ 85
A. INTRODUCTION... 85
B. OVERVIEW OF THE PROVISIONAL IRISH REPUBLICAN ARMY.. 86
C. TYPE II DESIGN STATE.. 87
1. High Hostility of the Environment 87
D. TYPE-II DARK NETWORK: RESTRICTIVE-ORGANIC 89

1. Restrictive Action 89
2. Organic Configuration 90
E. FUNDAMENTAL COMPONENTS 91
1. Directional Component 91
2. Operational Component 95
3. Supportive Component 96
F. CONCLUSION AND VULNERABILITIES 100

VI. TYPE-III DARK NETWORK: SELECTIVE-TECHNICAL 103
A. INTRODUCTION 103
B. OVERVIEW OF HEZBOLLAH 104
C. TYPE III DESIGN STATE 106
1. Moderate Hostility of the Environment 106
2. High Requirement for Secure Coordination of Work 107
D. TYPE III DARK NETWORK: SELECTIVE-TECHNICAL 108
1. Selective Action 108
2. Technical Configuration 108
E. FUNCTIONAL COMPONENTS 109
1. Directional Component 109
2. Operational Component 110
3. Supportive Component 112
F. VULNERABILITIES AND CONCLUSION 114

VII. TYPE-IV DARK NETWORK: SURGICAL-AD HOC 119
A. INTRODUCTION 119
B. OVERVIEW OF THE HAMBURG NETWORK 120
C. TYPE IV DESIGN STATE 121
1. High Hostility of the Environment 121
D. TYPE-IV DARK NETWORK: SURGICAL–AD HOC 124
1. Surgical Action 124
2. Ad Hoc Configuration 124
E. FUNDAMENTAL COMPONENTS 125
1. Directional Component 125
2. Operational Component 126
3. Supportive Component 128
F. VULNERABILITIES AND CONCLUSION 129

VIII. CONCLUSIONS AND RECOMMENDATIONS 133
A. A THEORY OF DARK NETWORK DESIGN 133
1. Environmental Hostility 134
a. Moderate Hostility 134
b. High Hostility 134
2. Secure Coordination of Work 134
a. Moderate Requirement for Secure Coordination of Work 135
b. High Requirement for Secure Coordination of Work 135

3. Adherence to the Principles of Dark Network Design 136

B. INSIGHTS FROM OUR RESEARCH 137

C. RECOMMENDATIONS FOR ILLUMINATION AND INTERDICTION 138

1. Understand and Change the Environment 138

2. Exploit External and Internal Network Misalignment 138

3. Develop Dark Counter-Networks 140

D. RECOMMENDATIONS FOR FURTHER STUDY 140

1. Use of Geospatial, Temporal, and Network Analysis Tools 140

2. Deep-Dive Each Design State 140

3. Research Gray Networks as Problems 141

4. Examine Unrestricted Dark Network Warfare 141

LIST OF REFERENCES 143

INITIAL DISTRIBUTION LIST 157

LIST OF FIGURES

Figure 1. The Nature of Networks 12
Figure 2. Galbraith Star Model of Organization Design. 17
Figure 3. Unaligned Organization Design 18
Figure 4. The Environment and Uncertainty 23
Figure 5. Mintzberg’s Components Applied to an Insurgent Organization 29
Figure 6. Assets and Facets of Networks 32
Figure 7. Basic Network Structures 36
Figure 8. Growth Model for Networks 39
Figure 9. Network Characteristics Based on Hostility 41
Figure 10. Illustration of Cut-out/Intermediary Visualized in Palantir 46
Figure 11. Basic Network Structures with Cut-outs 47
Figure 12. Operational Cells in Parallel Visualized in Palantir. 48
Figure 13. Intelligence Cells in Parallel Visualized in Palantir. 49
Figure 14. Auxiliary Cells in Series Visualized in Palantir. 50
Figure 15. Dark Network Typology 55
Figure 16. Dark Network Components 57
Figure 17. Dark Network System Model 63
Figure 18. Type-I Dark Network Quadrant 65
Figure 19. Illustration of Dark Network Components 73
Figure 20. Restrictive Organic Dark Network 85
Figure 21. Illustration of Dark Network Components 91
Figure 22. Illustration of PIRA Components Visualized in Palantir. 94
Figure 23. Type-III Dark Network Quadrant 103
Figure 24. Illustration of Dark Network Components 109
Figure 25. Type-IV Dark Network Quadrant 119
Figure 26. Illustration of Dark Network Components 125

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1. Sample of Network Measures Used in Social Network Analysis 34
Table 2. Network Adherence to Principles of Dark Network Design............... 136

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ASU	Active Service Unit
CIA	Central Intelligence Agency
COIN	Counterinsurgency
DNA	Dynamic Network Analysis
FARC	Revolutionary Armed Forces of Colombia
FBI	Federal Bureau of Investigation
GHQ	General Headquarters
GSJ	Global Salafi Jihad
ICE	Immigration and Customs Enforcement
IIRIRA	Illegal Immigration Reform and Immigration Responsibility Act
IRA	Irish Republican Army
IW	Irregular Warfare
JI	Jemmah Islamiyah
KSM	Khalid Sheikh Mohammed
LEA	Law Enforcement Agencies
MS-13	Mara Salvatrucha 13
OC	Officer Commanding
OPSEC	Operations Security
OPTEMPO	Operational Tempo
PIRA	Provisional Irish Republican Army
RUC	Royal Ulster Constabulary
SCW	Secure Coordination of Work
SNA	Social Network Analysis
TBA	Tri-Border Area
TUUH	Technical University of Hamburg-Harburg
UDA	Ulster Defense Force
UDF	Ulster Defense Force
UVF	Ulster Volunteer Force
UW	Unconventional Warfare

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

Ian: I would like to thank my wife, Mary, and my children, Christina, Josh and Taylor for their enduring love, support and understanding throughout our time here in Monterey and over the past 23 years of military service. Because of your unwavering support, I am able to persevere through difficult times. Additionally, I would like to thank all of the NCOs and my commissioned peers that showed me what right looked like and gave me the opportunity to challenge the status quo for the benefit of the Special Forces Regiment.

Carrie: I would like to express gratitude to family, especially my Mom and Dad, for their support and understanding. I never would be able successfully juggle all the tasks I give myself without you. I would also like to thank the love of my life, Mike, for his love and superman-like patience during this wonderful roller coaster life of ours.

Doug: I am indebted to my wife, Stori, for all her unwavering support and encouragement through this academic process, and being the most spot-on proofreader and math tutor in the Monterey peninsula. Thank you for being my partner in this wonderful adventure, and on all our adventures to come.

We would like to thank our advisors and professors at the Naval Postgraduate School for their insight, guidance, understanding, and patience. Finally, we recognize all of the students and staff of the Defense Analysis Common Operational Research Environment (CORE) Lab and appreciate all of their efforts as our active support cell.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

> If ignorant both of your enemy and yourself, you are certain to be in peril…if you know the enemy and know yourself, you need not fear the results of a hundred battles.[1]
>
> –Sun Tzu, 500 B.C.

A. PURPOSE AND SCOPE

The purpose of this study is to create a theory of dark network design. Dark networks are networks that must remain hidden in order to achieve their purpose. Dark network design refers to the process by which a dark network configures its structure, component parts and sub-systems, and coordinates its activities in response to environmental changes.[2] While a wealth of literature from experts in the field of business management, such as Mintzberg and Galbriath, exists on designing and optimizing hierarchal organizations, there is little to no literature to help us understand dark network design. This study seeks to fill the gap in the current literature. In particular, we address two fundamental questions: 1) How are dark networks designed? 2) What are their vulnerabilities?

Our theory is based on concepts derived from the field of organizational theory. In particular, we use organizational design theory to identify two critical dimensions driving dark network design: the level of hostility in the environment and the requirement for secure coordination of work. We posit that these two dimensions produce four dark network configurations or designs: Type-I: Opportunistic-Mechanical; Type-II: Restrictive-Organic; Type-III: Selective-Technical; and Type-IV: Surgical-Ad hoc. Using open source data, we identify examples of dark networks that are representative of each of the design states.

[1] Sun Tzu, *The Art of War*, trans. Samuel B. Griffith (London: Oxford University Press, 1971), 84.

[2] Derived from Henry Mintzberg, *Mintzberg on Management: Inside Our Strange World of Organizations* (New York: The Free Press, 1989), 94.

We submit that each dark network design represents an ideal type that maximizes network output and minimizes the potential for interdiction. To the extent a dark network does not configure itself to protect itself from hostility in its environment or it violates requirements for secure coordination of work, it will be vulnerable to interdiction.

Studying networks that are designed to remain hidden using unclassified data presents some unique challenges. In his paper *Mapping of Networks of Terror Cells*, Valdis Krebs encountered the same challenges that criminal network analyst Malcolm Sparrow found a decade earlier when applying social network analysis to criminal activity: incomplete data, fuzzy network boundaries, and the dynamic nature of networks.[3] These problems are compounded when limiting research to open source data and keeping discussion of material at the unclassified level.

However, keeping our study on dark networks unclassified with an unlimited distribution has its advantages. Our conclusions are exportable to the classified domain and later can be operationalized by security services. Additionally, by avoiding discussion and specificity about operational tradecraft, we minimize the potential that dark networks could use our work to counter interdiction efforts. And finally, an unlimited distribution allows others to continue this research in the hope that it ultimately leads to greater efforts to illuminate and interdict dark networks on a global scale.

B. APPLICABILITY

The first decade of the 21st century presented the United States and its global partners a wide array of complex security challenges. Globalization and advances in technology have not only increased opportunities for peaceful growth and cooperation, but have also empowered an adaptive and resilient enemy that remains determined to use any means available to achieve its

[3] Malcolm K. Sparrow, "The Application of Network Analysis to Criminal Intelligence: An Assessment of the Prospects," *Social Networks* 13 (1991): 251–274 and Valdis E. Krebs, "Mapping Networks of Terrorist Cells," *Connections* 24 (2001): 43–52.

ideological objectives. On September 11, 2001, Mohammed Atta's Hamburg network, an affiliate of the al-Qa'ida social movement global Salafi jihad, launched the deadliest attack ever on American soil that became an iconic event in the protracted struggle between conventional superpowers and a dynamic transnational irregular threats.[4] This dark network enabled 19 hijackers to defeat the elaborate security mechanisms of the United States and deliver a decisive blow to America by using airplanes as weapons of mass destruction. In this deadly asymmetric attack, the hijackers killed close to 3,000 people in a matter of hours and arguably redefined the nature of warfare, as we know it. Although the U.S. and its partners managed to topple the Taliban regime, the dark terrorist networks of al-Qa'ida and the global Salafi jihad persist today. Dr. John Arquilla explained the resilience of terrorist organizations in his testimony before the House Armed Services Subcommittee on Terrorism, Unconventional Threats and Capabilities in 2008:[5]

> The terrorists remain on their feet and fighting, in large part because their nimble, networked structures have been given the opportunity to keep developing, their hallmarks being the decentralization of authority, the proliferation of small cells throughout the world, and an abundance of lateral links—many in cyberspace—among and between their many nodes. They have developed a highly evolved, battle-tested variant of the classic network concept of operations: 'small pieces, loosely joined.'

Some nine years after the 9/11 attacks that triggered a vast expenditure of U.S. national treasure, President Barack Obama reaffirmed an ongoing U.S.

[4] According to Marc Sageman, al-Qa'ida has two dimensions: a social movement and an organization. Al-Qa'ida a social movement for the global Salafi jihad that is composed of informal networks that mobilize people to resort to terrorism. Al-Qa'ida as an organization makes reference to a formal structure of power, authority, and source of material support and tends to refer to "central leadership" that frames that strategic message and vision that provides direction and capacity for the global Salafi jihad. See Marc Sageman, *Understanding Terror Networks*, Philadelphia: University of Pennsylvania Press, 2004 and Marc Sageman, *Leaderless Jihad: Terror Networks in the Twenty-First Century*, Philadelphia: University of Pennsylvania Press, 2008.

[5] John Arquilla, "It Takes a Network: On Countering Terrorism," *United States House of Representatives*, September 18, 2008, http://armedservices.house.gov/pdfs/TUTC091808/Arquilla_Testimony091808.pdf (accessed October 20, 2010).

commitment to “disrupt, dismantle, and defeat al-Qa’ida and its violent extremist affiliates in Afghanistan, Pakistan, and around the world.”[6] Like a malignant cancer, dark networks like al-Qa’ida continue to metastasize in the pursuit of their nefarious goals, all the while depleting the energies of the nations that oppose them. A dark network of criminal organizations, violent extremist, state and non-state sponsors of terrorism, and other illegal entities continue to identify and exploit vulnerabilities in their surrounding environment.[7] Additionally, these entities build local, regional, and transnational alliances that yield a global dark network of state and non-state actors that could potentially wage “Unrestricted Warfare” against the United States and its allies.[8] Although the United States undoubtedly considers itself the premier fighting force in the world, based on technological and firepower superiority, dark networks that have relatively few resources and limited technology continue to wear away American lives, national treasure, morale, and political will.

We concur with network researcher Manuel Castells who states that “networks matter” because they are the underlying structure of our lives.[9] Through advances in technology, they allow social and knowledge networks to reconfigure themselves on a global-scale to permeate all domains of life, creating a networked society. We also believe Castells’ argument is applicable to the

[6] Barack Obama, "National Security Strategy," *The White House*, May 27, 2010, www.whitehouse.gov/sites/default/files/rss.../national_security_strategy.pdf (accessed May 28, 2010).

[7] Dark networks have the potential to create or exacerbate unstable environments. See Bryan Martin, Gabriel Szody and Joshua Thiel, *Radical Destabilization: A Low Cost, High Success Policy Option for the United States*, Master's Thesis (Monterey: Naval Postgraduate School, 2010).

[8] “Unrestricted Warfare” is modified combined warfare that goes beyond limits and is driven by the principals of omnidirectionality, synchrony, limited objectives, unlimited measures, asymmetry, minimal consumption, multidimensional coordination, and adjustment and control of the whole process. See Qiao Liang and Wang Xiangsui, "Unrestricted Warfare," *IWS - The Information Warfare Site*, PLA Literature and Arts Publishing House, February 1999, http://www.iwar.org.uk/iwar/resources/china/iw/unrestricted-warfare.pdf (accessed October 7, 2009).

[9] Manuel Castells, “Afterward: Why Networks Matter,” in *Network Logic: Who Governs in an Interconnected World?*, ed. Helen McCarthy, Paul Miller and Paul Skidmore, 221–225 (London: Demos, 2004).

national security setting and is reflected in the works of RAND researchers John Arquilla and David Ronfeldt on the topic of "Netwar."[10] Network theories of Castells, Arquilla, and Ronfeldt support the nature of the global struggle against violent extremism and provide a basis for our claim that "dark networks matter." While the U.S. cannot disregard the importance of remaining on the cutting edge of technology an innovating new strategies to wage conventional war with other nation states, recent history reveals that it is critical to have the capacity to identify, understand, and defeat dark networks that pose a threat to U.S. national security.

C. THE NATURE OF DARK AND LIGHT NETWORKS

1. Definitions

To introduce dark networks and their domains, we begin with an overview of networks. Networks are defined as "a set of actors connected by a set of ties."[11] They are "open structures with a set of interconnected nodes that are able to expand without limits, integrating new nodes as long as they are able to communicate within the network … [and] they share the same communication codes, such as values or performance goals."[12]

A network can consist of formal or informal ties between nodes. These ties vary in type; examples include friendship or kinship ties, finance and business ties, etc. A set of ties of a particular type, such as friendship or kinship, represents a social relation and each relation defines a different network.[13]

[10] John Arquilla and David Ronfeldt, "The Advent of Netwar," *RAND Corporation*, 1996, http://www.rand.org/pubs/monograph_reports/MR789/ (accessed November 5, 2009) and John Arquilla and David Ronfeldt, "Networks and Netwars: The Future of Terror, Crime, and Militancy," *RAND Corporation*, 2001, http://www.rand.org/pubs/monograph_reports/MR1382/ (accessed November 5, 2010).

[11] Stephen P. Borgatti and Pacey C. Foster, "The Network Paradigm in Organizational Research: A Review and Topology," *Journal of Manangement* 29, no. 3 (2003): 991-1013, 992. For the purpose of this study, we use the terms actors, nodes, and entities interchangeably when referring to individuals or collective groups that are parts of a network.

[12] Manuel Castells, *The Rise of the Network Society* (Cambridge: Blackwell Publishers, 1996), 470.

[13] Castells, *The Rise of the Network Society*, 992.

Networks have a multitude of beneficial aspects and are undoubtedly the fabric of an interconnected society, but there are those actors that exploit the power of networks to achieve their illicit purposes.

For the purpose of this study, we define dark networks as interdependent entities that use formal and informal ties to conduct activities that may be perceived as illegal by an external entity and employ operational security measures and/or clandestine tradecraft techniques through varying degrees of overt, or more likely covert activity to achieve a purpose.[14] "Legality" is a matter of perception and can be interpreted differently by advocates or opponents of a dark network. While a dark network that is conducting unilateral covert operations for reasons of national security may be legal in the eyes of the sponsoring nation, those actions may violate legal statutes or be perceived as illegal by opponents of the same dark network. Because of its "illegal" nature, the dark network must become "invisible" to avoid illumination and interdiction. We do not use the moral or ethical justness of the network's purpose to define its shade. The battle between the forces of good and evil is problematic and beyond the scope of this study.

Because they participate in clandestine and covert activity, dark networks have the following characteristics:[15]

[14] Raab and Milward define dark networks simply as "as simply "illegal and covert"," as stated in Jorg Raab and H. Brinton Milward, "Dark Networks as Problems," *Journal of Public Administration Research and Theory* 13, no. 4 (October 2003): 413–439. This definition is bounded and problematic because legality can be interpreted differently between the sponsor and the opponent of a dark network. Furthermore, covert activity – hiding the sponsor of an act – is distinctly different from clandestine activity – hiding the presence of and act. For more information on the nuances of clandestine and covert activities, see James McCargar, "Part 1: Fundementals and Forms of Action," in *A Short Course in the Secret War*, 15–151 (Lanham: Madison Books, 2001).

[15] Derived from Andrew R. Molnar, Jerry M. Tinker and John D. LeNoir, "Chapter 1: Underground Organization within Insurgency," in *Human Factors Considerations of Undergrounds in Insurgencies*, 17–35 (Washington, D.C.: Special Operations Research Office, 1965).

- Their goals are often illegal under the system within which they exist or intend to operate;
- Their activities may be either legal or illegal, but they tend to use illegal means to achieve their goals;
- They attempt to conceal the identity of their members from the governing authority.

Understanding how dark networks are configured to achieve their purpose will allow us to develop counter-network strategies to check their advances and take advantage of their vulnerabilities.

In contrast to dark networks, light/bright networks are undeniably legal and can operate openly, with minimal security considerations. Their legal status maximizes the potential for collaboration and minimizes the requirement for secure coordination of work. A third type of network, which we identify as "gray networks," is suggested in *Dark Networks as Problems*. The authors Jorg Raab and H. Brinton Milward, found that dark networks are often connected to the legal networks that were trying to destroy them.[16] These "gray" networks result when vetted-witting actors from dark networks use deception and elaborate security measures to misrepresent their true intent in order to manipulate unvetted-unwitting actors of light/bright networks.[17] Their domain thus consists of front organizations and other pseudo-groups that misrepresent their true intent to serve as platforms for dark networks to penetrate and exploit legal aspects of light/bright networks.[18] They manifest themselves through a myriad of activities executed by state and non-state sponsored dark networks, such as organized

[16] Raab and Milward, "Dark Networks as Problems," 413–439.

[17] By our definition, vetted actors are those actors that, through some process of validation, are perceived as "trusted agents" by entities within the network; and witting actors are those actors that have full knowledge of the true purpose of their actions. Unvetted and unwiiting actors are the opposite.

[18] For more information on how pseudo-groups and pseudo-operations are conducted during for counter-insurgency operations, see Lawrence E. Cline, "Pseudo Operations and Counterinsurgency: Lessons from other Countries," *United States Army War College Strategic Studies Institute*, June 2005, http://www.carlisle.army.mil/ssi/pubs/display.cfm?PubI D=607 (accessed November 8, 2009) and Edgar A. Jimenez, James S. McCullar and Kevin M. Trujillo, *Pseudo Operations and Deception in Irregular Conflict*, (Monterey: Naval Postgraduate School, 2010).

criminal syndicates, insurgent groups, violent extremists, and transnational terrorist groups that infiltrate and exploit legal networks for nefarious purposes. Although the legal status of a network provides a broad criterion for determining the network's "shade," it does not offer the granularity required to determine network typology. Next, we offer exogenous and endogenous dimensions that are useful in comparing and contrasting networks.

2. Dimensions to Compare and Contrast Networks

Two dimensions are useful in comparing and contrasting light/bright, gray, and dark networks: the level of hostility in the environment and the level of security required for the secure coordination of work.

a. Hostility of the Environment

Hostility of the environment is any external factor that can negatively affect the network in pursuit of its purpose. In a business setting, Covin and Slevin found:[19]

> Hostile environments are characterized by precarious industry settings, intense competition, harsh, overwhelming business climates, and the relative lack of exploitable opportunities. Non-hostile or benign environments, on the other hand, provide a safe setting for business operations due to their overall level of munificence and richness in investment and marketing opportunities.

A light/bright network faces a low level of hostility and is typically only concerned with surviving in the competitive market place and achieving its purpose. Although the external environment can have negative affects on the network, the level of hostility is low when compared to that of dark networks. Dark networks must overcome the challenges that affect light/bright networks, plus the additional constraints of remaining hidden. They not only have to remain competitive and achieve their purpose in a turbulent and precarious marketplace,

[19] Jeffrey G. Covin and Dennis P. Slevin, "Strategic Management of Small Firms in Hostile and Benign Environments," *Strategic Management Journal* 10 (1989): 75–87.

but also do so with the constant threat of destruction by external opposition elements, such as state security forces and rival networks. A high level of hostility in the environment may not only keep a dark network from achieving its purpose, but could potentially destroy it.

b. Secure Coordination of Work

Secure coordination of work is the implementation of countermeasures to protect the network from outside threats as it directs its different components to achieve its purpose.[20] Light/bright networks operate in an environment that is less hostile than that of their dark counterparts, thus they have low requirements for secure coordination of work. On the other hand, dark networks have a high requirement for secure coordination of work and must exhibit clandestine and covert behavior to avoid illumination and interdiction by opposition elements. Clandestine behavior, concealing the existence of an operation, and covert behavior, concealing the sponsor of an operation, requires dark networks to commit additional resources to establish structural and relational mechanisms that provide secure coordination of work.[21]

3. Network Types

Combining the two aforementioned dimensions, hostility of the environment and secure coordination of work, we can differentiate among the three types of networks: dark, light/bright, or gray.

[20] For further details on coordination of work, see Andrew H. Van De Ven, Andre L. Delbecq and Jr., Richard Koenig, "Determinants of Coordination Modes within Organizations," *American Sociological Review* (American Sociological Association) 41, no. 2 (April 1976): 322-338 and J. Michael Steele, "Models for Managing Secrets," *Management Science* (INFORMS) 35, no. 2 (1989): 240-248.

[21] Techniques of clandestine and covert behavior drive organizational devices, patterns of communications, and rigid security procedures. See Andrew R. Molnar, Jerry M. Tinker and John D. LeNoir, "Chapter 5: Clandestine and Covert Behavior," in *Human Factors Considerations of Undergrounds in Insurgencies*, 101–108 (Washington, D.C.: Special Operations Research Office, 1965).

a. Dark Networks

Dark networks are typified by a high level of hostility in the environment and a high requirement for secure coordination of work. Members of dark networks are vetted and witting to the true nature of their illegal activities and the illegal status of the network.

b. Light/Bright Networks

Light/Bright networks are typified by a low level of hostility in the environment and a low requirement for secure coordination of work. Hostility is low, but not absent. Thus, light/bright networks may apply security measures to buffer hostility by making themselves a hardened target, but not to hide the presence of the network. Actors in light/bright networks may be vetted or unvetted, and are witting to the true nature of their activities and the status of the network.

c. Gray Networks

Gray networks are products of the fuzzy domain where dark and light/bright networks interact. Vetted-witting actors from dark networks use deception and elaborate security measures to misrepresent their true intent in order to manipulate unvetted-unwitting actors of light/bright networks. Since gray networks are an evolutionary byproduct that occurs through the bridging of the potential space between light/bright and dark networks, they have the broadest range of possible external and internal situations.

Because of their interconnectivity with dark and light/bright networks, gray networks may operate in a domain typified by a moderate-high level of hostility, but still have a moderate-low requirement for secure coordination of work based on the purpose and the of the network and its use of advance technology.[22] Gray networks of this domain tend to be technology-based and exploit ill-governed/ungoverned spaces to avoid illumination and interdiction.[23]

Likewise, a gray network can function in a benign environment, but still employ a moderate-low to moderate-high level for secure coordination of work to keep illicit activities hidden from unwitting members of the light/bright network and opposition security forces.[24] Political and commercial fronts are the infrastructure that facilitates this exploitation of the licit world to support illicit activity.[25] In the context of unconventional warfare, the underground and auxiliary elements of a resistance organization will develop gray networks in their organization and build-up phase to remain undetected while they build capacity

[22] For example, cyber-criminals that develop and employ cutting-edge techniques to embezzle funds through the surreptitious exploitation of a highly technical process that is extremely difficult to detect. These crimes present a hostile environment due to their illegal nature, but may—at the time—require moderate-low secure coordination of work. This is because the target of the cyber-attack or criminal investigators may be unaware that a crime was committed, or not have the capacity to detect and/or counter the technology used to conduct the crime.

[23] For more information on ill-governed and ungoverned spaces, see Angel Rabasa et al., "Ungoverned Territories: Understanding and Reducing Terrorism Risks," *RAND*, 2007, http://www.rand.org/pubs/monographs/2007/RAND_MG561.pdf (accessed October 12, 2009); Cristina Brafman Kittner, "The Role of Safe Havins in Islamist Terrorism," *Terrorism and Political Violence* 19, no. 3 (2007): 307—327; Anna Simons and Davis Tucker, "The Misleading Problem of Failed States: A 'Socio-geography' of Terrorism in the Post-9/11 Era," *Third World Quarterly* 28, no. 2 (2007): 387—401; and Prager Security International, *Denial of Sanctuary: Understanding Terrorist Safe Havens*, ed. Michael Innes (Westport: Prager Security International, 2007).

[24] For example, social movements tend to operate within the legal framework to resolve their issues and voice their collective concerns in accordance within the accepted norms of society. This tends to form light/bright networks that become the legitimate face of defection from the status quo. If the means or timeline for change does not satisfy the members that are highly committed to achieving the network’s purpose, splinter groups will form and form dark networks with a radical ideology. These dark networks exploit the original movement and leverage it as a means of ideological and material support to conduct illegal activity and achieve a purpose.

[25] Islamists often use strategic communication to frame their ideology in a manner to evoke emotional support to their cause. This sets the conditions for dark networks to use fronts to obtain active and passive support for the Salafi jihad. For an example of this rhetoric, see Anwar al-Alwaki, "44 Ways to Support the Jihad," *The Force of Reason*, November 2009, http://theforceofreason.com/wp-content/uploads/2009/11/44-Ways-to-Support-Jihad.pdf (accessed June 2, 2010).

for the eventual overthrow of the standing government.[26] The nature of the interwoven relationships of dark, light/bright, and gray networks is graphically represented in the nature of networks (Figure 1). Although gray networks are problematic and present challenges to security and stability, they are not our focus in this study. We focus on dark networks where the environmental hostility is high and there is a high need for the secure coordination of work.

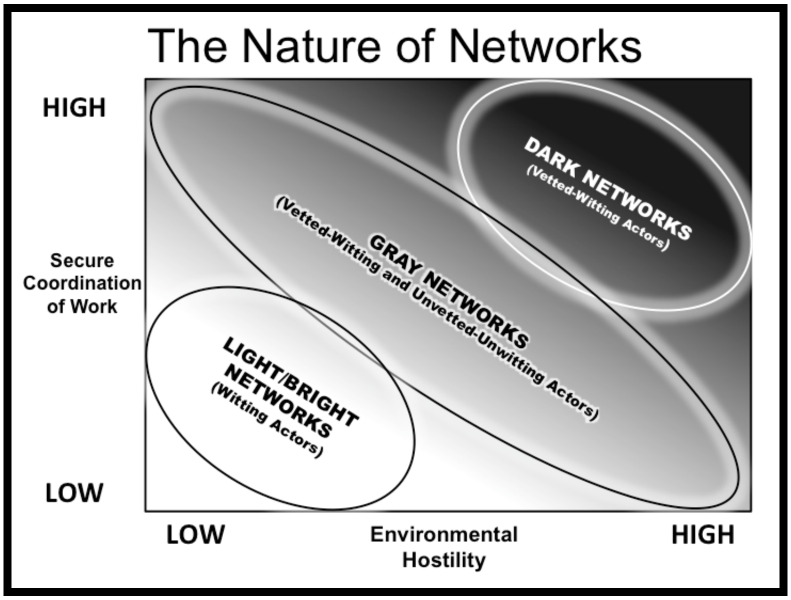


Figure 1. The Nature of Networks

D. IMPACT OF THE STUDY

This study develops a theory of dark network design. Understanding how dark networks are designed, provides a conceptual construct for the interdiction

[26] The U.S. Department of Defense defines unconventional warfare (UW) as activities conducted to enable a resistance movement or insurgency to coerce, disrupt or overthrow and occupying power or government by operating through or with and underground, auxiliary and guerrilla force in a denied area. Although theory on UW, counterinsurgency (COIN), and other forms of irregular warfare (IW) is beyond the scope of this study, we argue that current doctrine must take a network approach to understanding resistance warfare. See Mark Grdovic, "SWCS PUB 09-1: A Leader's Handbook to Unconventional Warfare," *United States Army John F. Kennedy Special Warfare Center and School*, November 2009, http://www.soc.mil/swcs/swmag/Assets/SWCS%20Publications/Leaders%20Guide%20Final.pdf (accessed January 27, 2010) and Department of Defense, "Irregular Warfare: Countering Irregular Threats," Vers. 2.0, *United States Joint Forces Command Joint Operating Concepts*, May 17, 2010, http://www.dtic.mil/futurejointwarfare/concepts/iw_joc2_0.pdf (accessed June 22, 2010).

of malignant dark networks that pose a threat to global security. Our theory also provides a basis for developing counter-networks to defeat traditional and irregular threats that are prevalent in today's turbulent security environment. Developing these sanctioned clandestine mechanisms for covert action will allow us to adopt a proactive, rather than reactive, posture toward dark networks. Identifying and exploiting the vulnerabilities of an opposition dark network while simultaneously developing safeguards to mitigate vulnerabilities in our own networks epitomizes Sun Tzu's tenant of knowing ourselves and knowing our enemy. This study presents the theoretical framework for the deliberate design, analysis, and interdiction of dark networks.[27]

E. THESIS ORGANIZATION

Chapter II reviews the organization theory literature and provides the foundation of our theory of dark network design. We derive concepts from the field of organizational design and current research on both light/bright and dark networks. These fields of study enable us to outline two design challenges: protection against external hostility and coordination of work to achieve a purpose. This body of knowledge informs our analytical framework for our theory of dark network design in the next chapter.

Chapter III introduces our theory of dark network design. First, we show how the relative hostility of the environment and the network's requirement for the secure coordination of work determine its design state. Second, we introduce our theoretical model that yields four design states and typological configurations of dark networks: Type-I: Opportunistic-Mechanical; Type-II: Restrictive-Organic; Type-III: Selective-Technical; and Type-IV: Surgical-Ad hoc. Third, we introduce our model that identifies the three fundamental components

[27] To learn more about the latest tools, concepts, and methodology for illuminating and interdicting dark networks, visit The Naval Postgraduate School Common Operational Research Environment(CORE) Lab (http://www.nps.edu/research/CoreLab/index.html); Palantir Technologies (http://www.palantir.com/); Steve Borgatti (http://www.steveborgatti.com/ and http://www.analytictech.com/); Pajek (http://vlado.fmf.uni-lj.si/pub/networks/pajek/); and The Center of Computational Analysis of Social and Organizational Systems (CASOS) at Carnegie Melon University (http://www.casos.ece.cmu.edu).

of a dark network: directional, operational, and supportive. Fourth, we present the two challenges to dark network design: buffering hostility and coordinating work to produce output. To overcome these challenges, dark networks strive to adhere to the six principles of dark network design: security, agility, resilience, direction setting, control, and capacity. Finally, we will introduce our dark network system model that illustrates how a dark network coordinates work in a hostile environment to produce output and achieve its purpose.

Chapters IV, V, VI, and VII present illustrative examples of each of our four dark network configurations. These examples are Mara Salvatrucha-13 (MS-13), The Provisional Irish Republican Army (PIRA), Hezbollah, and the Hamburg network that conducted the 9/11 attacks. We analyze against their design states and the principals of dark network design to identify potential vulnerabilities.

Finally, Chapter VIII summarizes our theory of dark network design, provides recommendations for illuminating and interdicting dark networks, and offers areas for future research. Undoubtedly, this study will generate more questions than it answers and will serve as a catalyst for further research to develop concepts related to network warfare.

II. LITERATURE REVIEW

A. INTRODUCTION

Chapter I introduced the purpose and scope of the study, general concepts related to the nature of networks, and why dark networks matter. The purpose of this chapter is to review pertinent literature on organizational design and network research in order to identify the basic elements of dark network design. We begin with a review of literature to identify the basic features of organizational design. Next, we summarize current bodies of knowledge pertaining to light/bright and dark networks that address their structure and relationships. Finally, we identify gaps in the current literature on network design.

B. ORGANIZATION DESIGN

Organization design theory provides a starting point for the development of a theory of dark network design. A premise of organization theory is that when people come together to achieve a common goal, they form an organization. According to Daft, organizations are: 1) social entities, 2) goal directed, 3) designed as deliberately structured and coordinated activity systems, and 4) linked to the external environment.[28] A variety of organizations exist, ranging from small and regional to large and multinational. Daft states, "[the] key element of an organization is not a building or a set of policies and procedures; organizations are made up of people and their relationships with one another."[29] Daft's statement highlights the idea that an organization is the sum of all its parts: the people, their interactions (both with each other and with the environment), goals, customers, suppliers, processes, and policies—the list goes on. Most

[28] Richard L. Daft, *Organizational Theory and Design*, 8th Edition (Madison: South Western Educational Publishing, 2003), 11.

[29] Daft, *Organizational Theory and Design*, 11.

importantly, Daft underscores the point that in order to survive, an organization must adapt and effectively design itself for its environment.[30]

Organization design is defined as the "deliberate process of configuring structures, processes, reward systems, and people practices and policies to create an effective organization capable of achieving the business strategy."[31] In his "star model", Jay Galbraith identifies five components of organization design: strategy, structure, processes and lateral capability, rewards systems, and people practices. Strategy is the cornerstone of the design process and sets the organization's direction through its vision, mission, market, and how the organization plans to compete within its market. Structure determines formal power and authority, reporting relationships, and roles within the organization. Processes and lateral capability address the organization's requirement for internal and external collaboration for information sharing and decision-making. Formal and informal networks, processes, teams, integrative roles, and matrix structures enable collaboration. Rewards systems that are based on goals, metrics, and evaluations instill positive organizational values and behaviors that are recognized with compensation and other rewards. People practices are the collective human resource that creates organizational capital and capacity. These include staffing and selection, performance feedback, and programs for learning and development. The interconnected and mutually dependent relationship of Galbraith's five components of organization design is depicted in the star model of organization design (Figure 2).

[30] Daft, *Organizational Theory and Design*, 13.

[31] Jay Galbraith, Diane Downey and Amy Kates, *Designing Dynamic Organizations* (New York: American Management Association, 2002), 2. They further state that organization "design" is often incorrectly used synonymously with organization "structure": "The organization design process and its outcome, however, are much broader than rearranging the boxes on an organization chart."

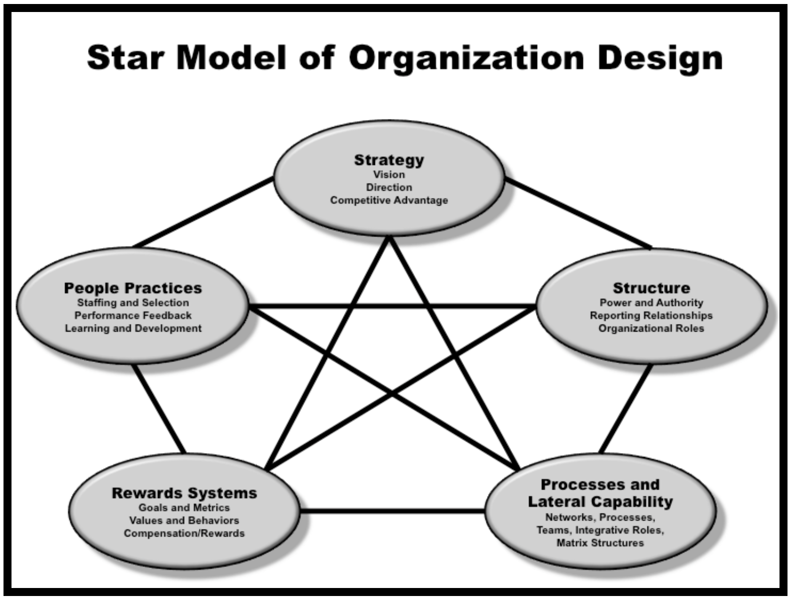


Figure 2. Galbraith Star Model of Organization Design.[32]

This model demonstrates that organizational design is not as simple as "rearranging boxes on the organization chart."[33] It is important to note that organizational design is *not* organizational structure. Organizational structure has three key components: (1) it designates formal reporting relationships, such as the organization's levels of hierarchy, (2) it identifies the groupings of individuals and/or departments, and (3) it includes the systems necessary for effective communication, coordination, and integration amongst departments.[34] At the very basic level, and example of organizational structure is a company's organization chart, while the organizational design is the dynamic combination of strategy, structure, processes, systems and people within the organization.[35]

Galbraith's heuristic star model shows that "just as in a living organism, if any of the components of the star are not attended to in the organization design

[32] Galbraith, Downey and Kates, *Designing Dynamic Organizations*, 2.

[33] Ibid., 2.

[34] Daft, *Organizational Theory and Design*, 86.

[35] Galbraith, Downey, and Kates, *Designing Dynamic*, 2.

process, the result is misalignment."[36] The consequences of misalignment can lead to confusion, friction, gridlock, internal competition, or poor performance and lead to unaligned organization design (Figure 3). The lack of a clear strategy leads to confusion that makes people in the organization pull in different directions and does not provide a basis for making decisions. If the structure is not aligned to the strategy, friction occurs leading to the inability to mobilize resources, ineffective execution, and loss of competitive advantage. Gridlock occurs if the development of coordinating mechanisms is left to chance. This leads to the lack of collaboration, prolonged decision and innovation cycle times, and difficulty with information sharing. If the rewards system does not support the organization's goals, internal competition occurs and ultimately leads to diffused energy, low standards, and turnover. Finally, if people are not empowered, low performance permeates the organization that results in diminished results and low employee satisfaction. Misalignment of the organization's design yields less than optimum performance.

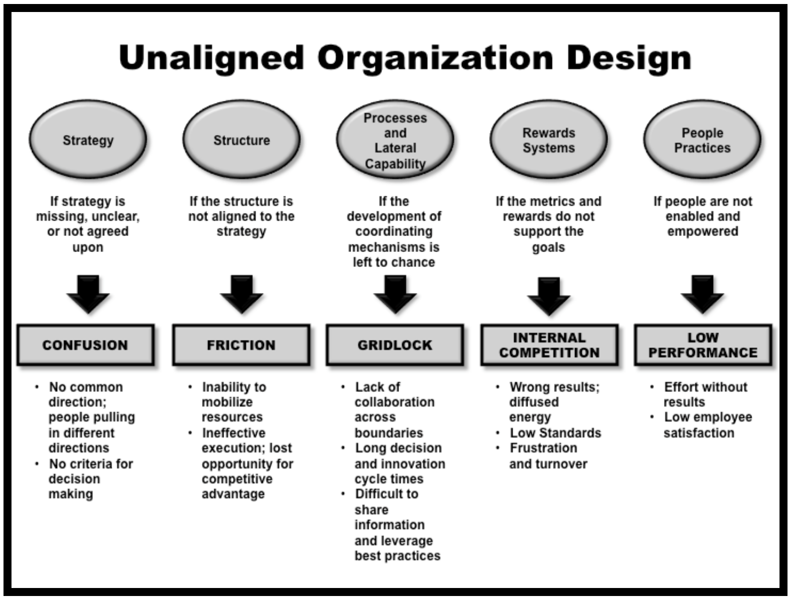

Unaligned Organization Design
Strategy
Structure
Processes and Lateral Capability
Rewards Systems
People Practices
If strategy is missing, unclear, or not agreed upon
If the structure is not aligned to the strategy
If the development of coordinating mechanisms is left to chance
If the metrics and rewards do not support the goals
If people are not enabled and empowered
CONFUSION
FRICTION
GRIDLOCK
INTERNAL COMPETITION
LOW PERFORMANCE
• No common direction; people pulling in different directions
• No criteria for decision making
• Inability to mobilize resources
• Ineffective execution; lost opportunity for competitive advantage
• Lack of collaboration across boundaries
• Long decision and innovation cycle times
• Difficult to share information and leverage best practices
• Wrong results; diffused energy
• Low Standards
• Frustration and turnover
• Effort without results
• Low employee satisfaction

Figure 3. Unaligned Organization Design[37]

[36] Galbraith, Downey, and Kates, *Designing Dynamic Organizations*, 2–4.

[37] From Galbraith, Downey, and Kates, *Designing Dynamic Organizations*, 4.

Other models also take a configurational approach to organization design. In *Organization Design: Fashion or Fit?*, Henry Mintzberg found that all organizations have a natural configuration, each a combination of certain elements of structure and situation.[38] He postulated that the purpose of configuration is to coordinate work and survive in a given setting. The external environment drives the organization to adapt its configuration or change the environment to achieve the organization's purpose. If an organization has the proper structure to achieve its purpose in the wrong environment, the organization may work to change the environment and preserve its structure. Mintzberg explains:[39]

> Essentially, the organization has two choices. It can adapt continuously to the environment at the expense of internal consistency-that is, steadily redesign its structure to maintain external fit. Or, it can maintain internal consistency at the expense of a gradual worsening fit with its environment, at least until the fit becomes so bad that it must undergo sudden structural redesign to achieve a new internally consistent configuration. In other words, the choice is between evolution and revolution, between perpetual mild adaptation, which favors external fit over time, and infrequent major realignment, which favors internal consistency over time.

In a Darwinian sense, survival is contingent on the organization's ability to understand its external environment and its internal structural and situational elements and find the appropriate configuration that fits its domain, or niche. Next, we will at some of the external and internal dimensions of organization design that affect configuration.

1. External Dimension: The Environment

Organizational researcher David Hanna posits that organizations are open systems that depend on their external environment for survival and are affected by influence and interaction with everything outside of its organizational

[38] Henry Mintzberg, "Organization Design: Fashion or Fit?," *Harvard Business Review* 59, no. 1 (January/February 1981), 103–116.

[39] Ibid., 115.

boundary.[40] This boundary is semi-permeable to allow for interaction with the environment to decrease uncertainty within the organization so that it can find the right fit between internal structure and the external environment.[41] The environment is all elements that exist outside the boundary of the organization, which includes people, other organizations, social and economic forces, and legal constraints and has the potential to affect all or part of an organization by providing opportunities, or imposing demands and constrains.[42] The sectors of the environment that directly impact the organization's ability to achieve its ends are known collectively as the task environment and those sectors that indirectly influence the organization are part of the general environment.[43] Uncertainty is the organization's lack of information about the environment that leads to difficulty in predicting external changes. Two dimensions of the environment determine the level of uncertainty: complexity and change.[44]

a. The Simple-Complex Dimension

The simple-complex dimension addresses environmental complexity. Complexity refers to the number and dissimilarity of external elements relevant that interact with and influence an organization. A simple environment may have as few as three or four similar external elements, while a complex environment will have more. An insurgency model serves as an example to explain complexity in the environment for both the insurgents and the counterinsurgents. From the perspective of the insurgents, a simple environment exists because the insurgents can conserve their resources and conduct decisive action on their terms to exploit the vulnerabilities of the state. Typically, the insurgents have a better understanding of the state's than the state knows about

[40] David P. Hanna, *Designing Organizations for High Performance* (Reading: Addison-Wesley Publishing Company, 1988), 8–9.

[41] Daft, *Essentials of Organization Theory and Design*, , 48–52.

[42] David Nadler, Michael Tushman and Mark B. Nadler, *Competing by Design: The Power of Organizational Architecture* (New York: Oxfor University Press, 1997), 29.

[43] Daft, *Essentials of Organization Theory and Design*, 47.

[44] Ibid., 52–53.

the insurgents. The insurgent's embeddedness in the population provides information superiority and decreases complexity. On the other hand, the counterinsurgents face a complex environment because they not only have to counter the actions of the insurgents, but they must also address interests of the population, various tribal or communal factions, competing political groups, organized criminal entities, and the influence of external actors in the conflict.

b. The Stable-Unstable Dimension

The stable-unstable dimension addresses dynamic change in environmental domain. A domain is stable if it remains the same over a period of months or years. Alternatively, environmental elements will shift abruptly in an unstable environment. An example of a stable domain would be a government that is well entrenched in society, exerts control over its sovereign territory, and maintains legitimacy in the eyes of a majority of the population. Change is evolutionary and occurs slowly over time. However, dynamic change creates an unstable environment and can occur when a government exerts little control over its territory and allows a multitude of competing interests to exert influence over the environment. This dynamic, unstable environment sets the conditions for revolutionary change and insurrection.

c. The Environment and Uncertainty

As stated previously, uncertainty comes in the form of the organization's lack of information about the environment. The level of uncertainty is related to the degree of complexity and change in the environment. Complexity and change in the environment affects organizational uncertainty and options for configuration and governance. Figure 4 illustrates how increasing environmental complexity and a loss of stability leads to an increase in uncertainty. As environmental complexity and uncertainty increases there is a corresponding need for organizations to increase decentralization and differentiation.[45]

(1) Level of Uncertainty

(a) LOW-LOW: This environment is also known as a simple-stable environment with a small number of external elements, all of which are similar, and the elements change slowly. Examples include: soft drink bottlers, beer distributers, container manufacturers, and food processors.[46]

(b) LOW-HIGH: This environment is also known as a complex-stable environment. In this environment there are a large number of external elements and those elements are dissimilar. These elements change slowly over time or remain the same. Examples include: e-commerce, fashion clothing, music industry, and toy manufacturers.[47]

(c) HIGH-LOW: This environment is known as a high-moderate uncertainty environment. This environment consists of small numbers of similar external elements in the environment, but these elements change frequently and unpredictably. Examples include: universities, appliance manufacturers, chemical companies, and insurance companies.[48]

(d) HIGH-HIGH: This environment is known as a complex-unstable environment. This environment consists of a large number of dissimilar external elements which change frequently and unpredictably. Examples include: Computer firms, aerospace firms, telecommunications firms, and airlines.[49]

[45] Mintzberg, “Organization Design: Fashion or Fit?,” 116.

[46] Daft, *Organization Theory and Design*,143

[47] Ibid.,143.

[48] Ibid.,143

[49] Ibid.,143

(2) Configuration Options. Complexity in the environment will determine the internal configuration of organizations. In simple stable environments organizations tend to utilize a mechanistic organization system that entails a clear hierarchy of authority, formalized internal organizations with codified rules and procedures.[50] In more dynamic environments organizations tend to toward an organic configuration, characterized by an adaptive, free flowing regulatory environment, with a decentralized authority structure.[51]

(3) Governance Options. Centralized organizations usually keep decision-making tied to a small cadre of individuals. This form of organizational governance is best for smaller organizations in simple environments. As organizations grow and environments become more complex, central leadership cannot effectively govern, and thus must decentralize authority to in order to adapt.[52]

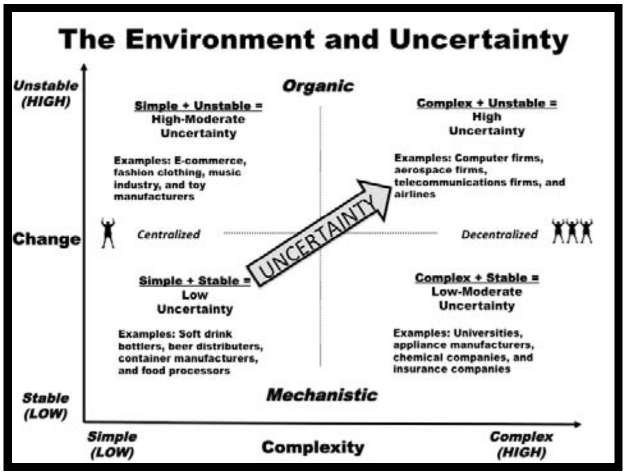

The Environment and Uncertainty
Unstable (HIGH)
Organic
Simple + Unstable = High-Moderate Uncertainty
Examples: E-commerce, fashion clothing, music industry, and toy manufacturers
Complex + Unstable = High Uncertainty
Examples: Computer firms, aerospace firms, telecommunications firms, and airlines
Change
Centralized
UNCERTAINTY
Decentralized
Simple + Stable = Low Uncertainty
Examples: Soft drink bottlers, beer distributers, container manufacturers, and food processors
Complex + Stable = Low-Moderate Uncertainty
Examples: Universities, appliance manufacturers, chemical companies, and insurance companies
Mechanistic
Stable (LOW)
Simple (LOW)
Complexity
Complex (HIGH)

Figure 4. The Environment and Uncertainty[53]

[50] Daft, *Organization Theory and Design*,143.

[51] Daft, *Organization Theory and Design*, 148.

[52] Steven McShane, Mary Ann Von Gilnow, *Organizational Behavior Essentials,* (Boston: McGraw-Hill, 2007), 237.

[53] Erik Jansen, "MN3121: Organizational Design for Defense Analysis" (Monterey: Naval Postgraduate School, Fall Term 2009).

In the next section, we discuss the Mintzberg configurations that rely heavily on their fit with the environment. The configuration's fit is directly related to level of complexity and stability in the environment. In a simple-stable environment, organizations are highly centralized and mechanistic. As the environment becomes more complex and dynamic, organizations become decentralized and organic to accomplish tasks. Thus, as the environment changes, the organization must adapt accordingly if it is going to efficiently coordinate work to achieve its purpose. In sum, the organization must be as dynamic as the task environment to achieve a proper fit.

2. Internal Dimension: Configuration

One concept presented by both organization and network experts is the importance of the role played by the environment in determining the configuration of an organization or a network.

a. Configuration

In the organizational sense, we define configuration as the visible manifestation of an organization's structural arrangement designed to achieve a purpose.

b. Mintzberg's Organizational Configurations

Organizational theorist Henry Mintzberg found that the characteristics of organizations fall in to natural clusters based on external and internal factors; these clusters yield seven natural organizational configurations that he described in terms of structure and situation: entrepreneurial, machine, professional, diversified, innovative, missionary, and political.[54]

(1) Entrepreneurial. Entrepreneurial organizations are simple, informal, flexible, and have little staff or hierarchy. The organization's

[54] For detailed information on each of the Mintzberg configurations, see Henry Mintzberg, *Mintzberg on Management: Inside Our Strange World of Organizations* (New York: The Free Press, 1989), 93–300.

power and authority resides with the chief executive who represents the organization's strategic apex and typically manages through direct supervision. These organizations fit in the simple-unstable environment and are highly agile because of their centralized management and organic structure.

(2) Machine. Machine organizations are centralized, bureaucratic, and rely on standardization of work processes to coordinate work. They rely on formal procedures, specialized and division of work, functional grouping, and extensive hierarchy. These organizations fit the simple-stable environment and are representative of mass services industries and governmental organizations.

(3) Professional. Professional organizations are decentralized bureaucracies that depend on the standardization of skills to coordinate work. The organization relies on the knowledge and skills of its professionals to produce output within the framework of the organization. These organizations fit the complex-stable environment and are exemplified by universities, hospitals, and other field that require technical expertise.

(4) Diversified. Diversified organizations–also know as divisional organizations–are market-based sub-components that are semi-autonomous mechanistic bureaucracies. Coordination is achieved through standardization of outputs and direction setting by middle managers. These organizations fit in the simple-stable environment and are typified by large corporations that produce a variety of products or across a geographically disbursed market.

(5) Innovative. Innovative organizations, which Mintzberg also refers to as adhocracies, are fluid, organic and selectively decentralized organizations that rely on subject matter experts to tackle complex projects. These projects tend to require extensive knowledge of cutting-edge technology

and rely on a bottom-up process of discovery to reach a resolution. These organizations coordinate work through mutual adjustment and fit in the complex-unstable environment.

(6) Missionary. Missionary organizations are directed by their adopted ideology that is grounded in a rich sense of values and beliefs and framed by charismatic leaders of the organization. The ideology provides a clear mission that inspires its members to pull together and coordinate work through a standardization of norms. Religious organizations are often, but not exclusively, missionary in nature and see a rise in their membership when the environment is complex-unstable. When a person feels the environment is uncertain and hostile, they tend to turn to religion to find answers. Mintzberg identifies three forms of missionary organization:

- Reformers, those who what to change the world directly;
- Converters, those who want to change the world indirectly; and
- Cloisters, those who do not seek to change the world, but to allow their members to pursue a unique lifestyle

(7) Political. Political organizations are focused on power, as opposed to structure. Politics tend to contradict coordination and cause disorder and disintegration within and organization. Generally, political organizations are focused on self-interests and cause the organization to pull apart. Mintzberg identified four forms of political organization:

- Confrontation, conflict that is intense, confined, and brief;
- Shaky alliance, where conflict is moderate, confined, and possibly enduring;
- Politicized organization, conflict that is moderate, pervasive, and possible enduring; and
- Complete political arena, conflict intense, pervasive, and brief.

c. Components of Configurations

In *Mintzberg on Management*, the presented the six basic parts (components) that are the building blocks of an organization's configuration: strategic apex, support staff, technical support, middle line, operating core, and the organization's ideology.[55]

(1) The Strategic Apex. The strategic apex is the top management and overseas the whole organization.

(2) The Middle Line. As the organization grows, the middle line becomes the link that ensures the work of the operating core is nested with the direction and vision of the strategic apex.

(3) The Operating Core. The base of the organization is the operating core and consists of the workers that produce the organization's products and render its services.

(4) The Technostructure. The technostructure performs the administrative and technical duties to plan and control the work of others.

(5) The Support Staff. The support staff executes the day-to-day internal activities that supports the organization as a whole and indirectly supports the output produced by the operation core.

(6) Ideology. Finally, the organization's ideology, directed by the strategic apex, defines the purpose of the organization and encompasses the traditions and beliefs that form the skeleton that guides all activities of the organization. Coordination mechanisms describe how the components of an organization coordinate their work.

d. Design Elements of Configurations

(1) Structural Design Elements. Structural design elements are: specialization of tasks, formalization of procedures, formal training and indoctrination needed for the job, grouping of units, size of the units, action

[55] Mintzberg, *Mintzberg on Management*, 95–115.

planning and performance control systems, liaison devices, vertical decentralization, and horizontal decentralization.

(2) Situational Design Elements. Situational elements are: an organization's age and size, technical system, internal and external environment, and distribution of power.

(3) Coordination Mechanisms. According to Mintzberg, coordination mechanisms are the most basic elements of structure and are the glue that holds and organization together.[56] He identifies six key means of coordination: mutual adjustment, direct supervision, standardization of work processes, standardization of outputs, standardization of skills, and standardization of norms. No organization can rely on one coordination mechanism, but some are optimum depending on the stage of the organization's life, its purpose, or its environment.

e. Summary of Configuration

Although Mintzberg's configurations are based on hierarchal organizations that operate in the light/bright world and do not directly export to network design, his premise that an optimal configuration is determined by the nature of the task environment is applicable to dark networks. In their thesis *Counter-Organization Targeting: Theoretical Framework for Analysis*, Daoust and Osborne applied Mintzberg's theory and applied it to a hierarchical insurgent organizational model to indicate which insurgent tasks fit into which basic component (Figure 5).[57] Although their model depicts a hierarchal organization, it helps define organizational elements related to direction, operations, and support that will be addresses later. Furthermore, the model illustrates the complexity of a hierarchal organizational structure based on its environment.

[56] Mintzberg, *Mintzberg on Management*, 101.

[57] Daniel C. Daoust and Joseph E. Osborne, *Counter-Organization Targeting: A Theoretical Framework for Analysis*, (Monterey: Naval Postgraduate School, 1996).

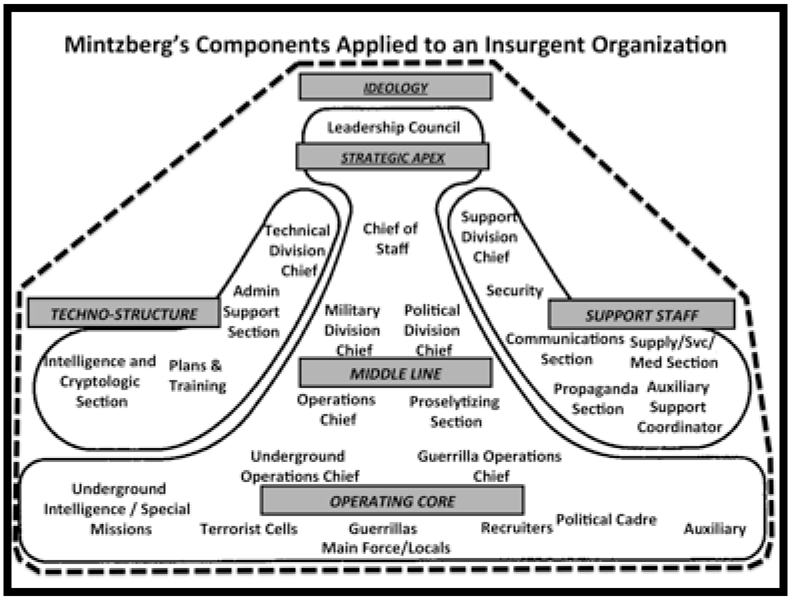


Figure 5. Mintzberg's Components Applied to an Insurgent Organization[58]

Organization design literature reveals that the way and organization configures itself to coordinate work according to its environment determines its ability to achieve its purpose in an efficient manner. When the organization's design does not fit with environment, it is inefficient and will waste time, resources, and is likely to fail to achieve its purpose. Relationships and structure enable the coordination of work. Next, we will examine current literature on network research to gain a better understanding of how light/bright, gray, and dark networks configure themselves in terms of the nature of relationships and structure to coordinate work in order to achieve a purpose.

C. NETWORK LITERATURE

As discussed in Chapter I, the nature of a network is based on its legal status and can be described as light/bright, dark, or when interconnected–gray. A light/bright network is overt and is able to maximize collaboration because it operates within the "legal framework of the states they act in."[59] On the other

[58] From Daoust and Osborne, *Counter-Organization Targeting,* 62.

[59] Raab and Milward, "Dark Networks as Problems," 4.

hand, dark networks are sometimes illegal and, whatever their ethical status, must adopt clandestine and covert behavior to avoid illumination by opposition elements seeking to destroy them. They operate in a hostile environment and that is inherently inefficient because of the tradeoff of secrecy and capacity to achieve its purpose. Where the two meet is the ambiguous domain of gray networks that is characterized by a continuous state of deceptive behavior by dark networks to manipulate light/bright networks. According to Milward and Raab, “legal and illegal networks sometimes come together in a gray zone or they are confronted with the fact that what is legal in one country is illegal in the other.”[60] Understanding the nature of a network is important for understanding the manner that it achieves it purpose.

1. Basic Features of Networks

To get a better understanding of how a purpose is achieved using the networked, vice hierarchical, form of organization, we will review the work network researcher Patti Anklam in her book *Net Work: A Practical Guide to Creating and Sustaining Networks at Work and in the World*. While the studies of networks can be an abstract concept and problematic, Anklam provides key features for understanding networks. She argues that networks are complex adaptive systems of human relationships and that everyone in the network influences the outcome of the network. If it’s a network, you can draw it, it has and underlying purpose, and it creates value. Furthermore, all networks have a discernable purpose, structure, and leadership style.[61] Anklam’s insight help us look at the world through the network lens to see how network assets, facets, relationships, structure, governance, and design collectively interact to create value

[60] Raab and Milward, "Dark Networks as Problems," 5.

[61] Patti Anklam, *Net Work: A Practical Guide to Creating and Sustaining Networks at Work and in the World* (Burlington: Elsevier Inc., 2007), 4–7.

a. Network Assets

A network creates value through its relationships that are generated by the network's tangible assets known as capital and is responsible for achieving the network's intangible asset: purpose. The network produces value in the form of social capital that results from the interaction of the network's human, structural, and relational capital. *Human Capital* is derived from the knowledge, skills, and experience of the individuals required to provide solutions to customers. *Structural Capital* is produced as part of the network's internal procedures, processes, and internal organizational structures that have evolved to enable the organization to function as it does. *Relational Capital* is the value of a network's relationships with its customers, suppliers, and others it engages with to accomplish its business. Finally, the resulting *Social Capital* is the stock of active connections among people; the trust, mutual understanding, and shared values and behaviors that bind the members of human networks and communities and make cooperative action possible.

b. Network Facets

Network assets enable the four facets of networks: purpose, structure, style, and value. Purpose is what animates a network and causes its members to care about it. Structure reflects a network's form, the possible patterns and arrangement of the relationships; the assignment of roles and responsibilities within the networks; and the network's texture in terms of flexibility, strength, and density of social bonds. Style is the network's visible manifestation; the nature of the interactions in the network; its social climate, which includes culture, core values, and norms; the manner of interactions; the balance of its orientation towards results or discovery; and its leadership style. Purpose, structure, and style produce value: the tangible and/or intangible network output in direct alignment with its purpose. The assets and facets of networks (Figure 6) provide a framework designing networks produce value.

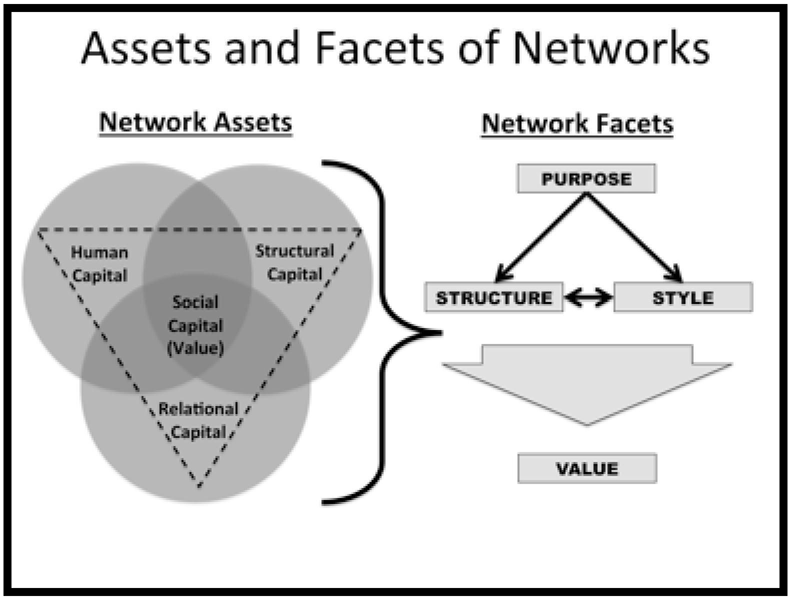


Figure 6. Assets and Facets of Networks[62]

c. Network Relationships

Social capital is contingent on the strength of relationships in the network to make cooperative action possible. The legal nature of light/bright networks allows them to build a robust set of ties in order to maximize collaboration and efficiently coordinate work to produce value and achieve a purpose.[63]

(1) Formal and Informal Ties. Relationships are measured by analyzing the formal and informal ties between actors, or nodes, based on similarities (location, membership, and attribute), social relations (kinship, other role, affective, and cognitive), interactions, and flows of tangible

[62] From Anklam, *Net Work*, 17, 30.

[63] The field of social network analysis often uses mathematical computations to determine a network's structure and assumes that interpersonal ties matter because they transmit behavior, attitudes, information, or goods. While techniques for using social network analysis to illuminate and interdict dark networks is beyond the scope of this study, social network theory provides an important foundation for understanding the nature of relationships in networks. Wouter de Nooy, Andrej Mrvar and Vladimir Batagelj, *Exploratory Social Network Analysis with Pajek* (Cambridge: Cambridge University Press, 2005).

and intangible assets.[64] In deeper detail, Everton finds that actors are linked together by ties that vary by their type and strength and include ties of sentiment (friendship, liking, respect); resources (business transactions, financial flows); association or affiliation (members of the same church, club, etc.); behavior (communication); geographic movement (migrations, physical mobility); status movement (social mobility); physical connection (road, river, or bridge connecting two points); formal ties (organizational hierarchy); and biological ties (kinship).[65] Using social network analysis tools, such as UCINET, Pajek, ORA and Palantir, analysts can measure and interpret the pattern of relationships of networks.[66] Common social network analysis measures (Table 1) are important for understanding the actor's place in the network. For light/bright networks, these measures are valuable for understanding information flow and identifying formal and informal leaders within the group and determining critical nodes related to the coordination of work. Similarly, these same measures can be used for illuminating and interdicting dark networks by identifying potential cut-points that can lead to network destabilization.[67]

[64] Stephen P. Borgatti, Ajay Mehra, Daniel J. Brass and Giuseppe Labianca, "Network Analysis in the Social Sciences," *Science* 323, no. 5916 (February 2009): 892-895.

[65] Sean F. Everton, *Tracking, Destabilizing, and Disrupting Dark Networks Using Social Network Analysis* (Monterey, CA: Naval Postgraduate School, 2009), 12.

[66] For more information on UCINET, Pajek, and ORA, see http://www.analytictech.com/, http://vlado.fmf.uni-lj.si/pub/networks/pajek/, http://www.casos.cs.cmu.edu/projects/ora/, and http://www.palantirtech.com/government respectively.

[67] Kathleen M. Carley, Ju-Sung Lee and David Krackhardt, "Destabilizing Networks," *Connections* 24, no. 3 (2001): 31-34.

Table 1. Sample of Network Measures Used in Social Network Analysis[68]

Network Measures	
Density	The total number of ties within a network divided by the total possible number of ties
Degree Centrality	The count of the number of an actor's ties.
Closeness Centrality	Based on the path distance, measures how close, on the average, each actor is to all other actors in the network.
Betweenness Centrality	Measures the extent to which each actor lies on the shortest path between all other actors in the network.
Eigenvector Centrality	Assumes that highly central actors are more important than ties to peripheral actors, so weights and actor's summed ties to other actors by their centrality scores.

(2) The Strength of Weak and Strong Ties. The strength of relationships, or ties, affects social capital. Mark Granovetter found that "weak" ties are more important that strong ties in terms of information flow because individuals with only a few weak ties will be deprived of information from distant parts of the social system and will be confined to the provincial views of their close friends and isolate them from the latest ideas that exist beyond their current clique.[69] Alternatively, David Krackhardt argues to the contrary that strong *philos* (Greek for friend) ties are important because they "constitute a base of trust that can reduce resistance and provide comfort in the face of uncertainty."[70] He adds that *philos* relationships are developed through interaction, affection, and time. Although weak ties may allow for better information flow, strong ties are crucial for network resilience and stability in the face of a volatile situation. Social capital built on trust ensures network

[68] Everton, *Tracking, Destabilizing, and Disrupting Dark Networks,* 109–125*.*

[69] Mark Granovetter, "The Strength of Weak Ties: A Network Theory Revisited," *Social Theory* I (1983): 201-233. p. 202.

[70] David Krackhardt, "The Strength of Strong Ties: The importance of Pilios in Organizations," in *Networks and Organizations: Structure, Form, and Action*, 216-239 (Boston: Harvard Business School Press, 1992). pp. 218-219.

survivability and the persistent pursuit of achieving a purpose. Another concept related to social capital the nature of an actor's strong and weak ties is that of structural holes.

(3) Structural Holes. Burt defines a structural hole as a relationship of non-redundancy between two actors that acts as a buffer to provide network benefits that are in some degree additive rather than overlapping.[71] A structural hole is related to efficiency of the network and is tied to Granovetter's theory on the strength of weak ties, both of which are applicable to relationships and structure in light/bright, gray, and dark networks. Next we will examine features of light/bright network structure.

d. Network Structures

Network structure is defined as the form and possible patterns and relationships within the network and includes the assignment of roles and responsibilities as well as the nature the social bonds of a network: the flexibility, strength and density.[72] In discussing network operational structures, John Arquilla and David Ronfeldt describe three fundamental forms of network structure that are based on how nodes interoperate with each other: 1) the chain network, where communications and resources must travel through intermediate nodes; 2) the star or hub network, where a set of actors are tied to a central actor or node and all communications must go through that actor; and 3) an all-channel or full-matrix network in which all the nodes are interconnected (Figure 7).[73] These basic network structures are often blended to in varying degrees to form hybrid network structures depending on the nature of the task environment.

[71] Ronald S. Burt, *Structural Holes: The Social Structure of Competition* (Cambridge: Harvard University Press, 1992), 65.

[72] Anklam, *Net Work,* 30.

[73] Arquilla and David Ronfeldt, *Networks and Netwars*, 7–8.

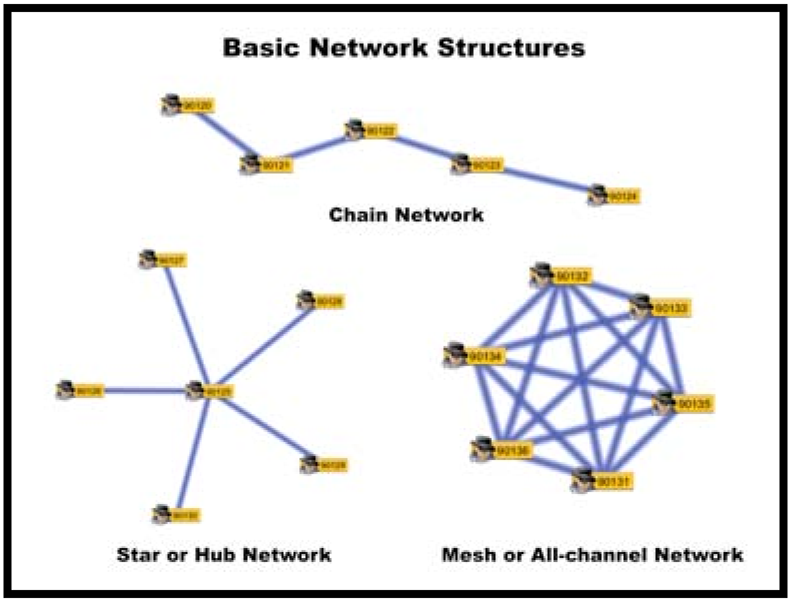


Figure 7. Basic Network Structures[74]

e. Network Governance

Anklam found that all networks have some form of governance, explicit or assumed, that keeps the organization in balance and relationships intact and is necessary for steering a steady operational state.[75] Management of membership is a critical governance task because it ultimately can shape the nature of the network's relationships, structure, and size. Anklam describes three types of network membership: open, criteria-based, and invitation-only.[76] These types of membership are applicable to all "shades" of networks.

(1) Open Membership. Open membership establishes norms and assumes that only those that have a serious intent on sharing the network's purpose will participate and that actors will contribute to in accordance with the purpose of the network. It is the least restrictive (least secure) of the three memberships and has the potential of creating the most "weak" ties. As mentioned earlier, weak ties are important for the dissemination of information

[74] After Arquilla and David Ronfeldt, *Networks and Netwars*, 7–8.

[75] Anklam, *Net Work,* 59.

[76] Anklam, *Net Work,* 68–72.

beyond and actor's normal sphere of influence. These tend to produce mass-networks with limited control measures in order to maximize collaboration and are essentially "leaderless".[77]

(2) Criteria-Based Membership. A network that is criteria-based establishes a minimum criterion for membership based on some attribute that is aligned with the purpose of the network. This may be profession, education, income, religion, ethnicity, gender, etc. Because members share some common attribute, they may form "strong" ties because of a shared relationship or interest and therefore build a baseline of trust.[78] These tend to have moderate control measures and reflect the norms of its membership. Criteria-based networks can be the optimum platform for developing gray networks based on the shared attributes between actors in the licit and illicit world as described in Chapter I. Additionally, the affinity between actors that are tied by similar attributes provides an inherent level of trust and acts as a means of security for a dark network and is a critical aspect of clandestine and covert behavior. This creates an environment that is conducive for identifying members that may be susceptible for recruitment into invitation-only networks.

(3) Invitation-Only Membership. The most restrictive—and most secure—type of membership is by invitation-only. This closed network is suited for maintaining the nature of interaction of members of the group with outside entities. This provides a level of secrecy and protection from outside influence and typically has some method of vetting to verify the trustworthiness of invited members. A greater level of trust leads to greater access to critical information and can has the potential of moving an actor from the periphery (edge) of a network to its core (center). The concept of invitation-only

[77] Technology has given rise to a host of decentralized communities that are tied by a common purpose without any central leadership, such as peer-2-peer networks and other entities that rely on a sense of trust and community. See Ori Brafman and Rod A. Beckstrom, *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations* (New York: Penguin Group, 2006).

[78] Stephen P. Borgatti and Daniel S. Halgin, "Analyzing Affiliation Networks," *Steve Borgatti*, ed. P. Carrington and J. Scott, 2004, http://www.steveborgatti.com/papers/bhaffiliations.pdf (accessed November 05, 2009).

membership based on a vetted level of trust is key for understanding how dark networks securely recruit new members from light/bright world and incrementally give them access to compartmented plans and operations.

f. Network Design

Network design is the process of creating structures and processes to produce value. According to Anklam's network growth model (Figure 8), networks proceed through adaptive phases that define its purpose, structure, and style in order to produce value. The four phases of the network growth model are: creation, design, growth, and performance.[79] Creation and design can be intentional by a centralized top-down process or it may be by discovery through a decentralized, bottom-up process. Network creation by intention or discovery is contingent on a shared interest or clear purpose between the members of the network. In the design phase, the networks defines and frames its purpose, identifies stakeholders, builds relationships, establishes structure and governance, defines membership criteria and norms, determines tempo, and establishes physical and virtual presence. During the growth phase, the network builds capabilities, capital, creates connections, and ties members to achieve the network's purpose and establish core values. The network maintains its tempo and equilibrium during the performance phase by coordinating work and adjusting to changes in the task environment. This growth cycle produces a dynamic situation that enables network resilience during turbulent times.

[79] Anklam, *Net Work*, 132–134.

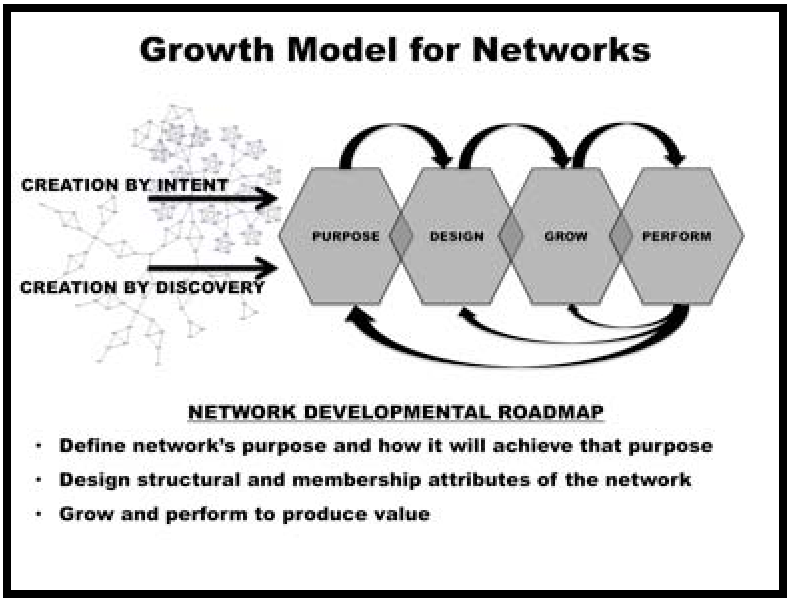

Growth Model for Networks
CREATION BY INTENT
CREATION BY DISCOVERY
PURPOSE
DESIGN
GROW
PERFORM
NETWORK DEVELOPMENTAL ROADMAP
• Define network's purpose and how it will achieve that purpose
• Design structural and membership attributes of the network
• Grow and perform to produce value

Figure 8. Growth Model for Networks[80]

Our understanding of network assets, facets, relationships, structure, governance, and design collectively interact to create value provides the foundation for understanding dark network design.

2. Dark Networks

The rise of the information age and the era of globalization has changed the environment in which war is fought. Dark networks, undergrounds, and any sort of clandestine or covert organization, face a conundrum. In order to achieve an objective, the network must become both expansive and aggressive. But in order to survive, they must take precautions and prize their security. Network patterns and size must be juggled so as to achieve an optimum balance between the need to expand and the need to maintain security. As McCormick and Owens found, the effectiveness of an underground organization is a function of operational capacity and security; performance depends on the organizational size and level of coordination; and its goal must be to achieve the highest operational impact given the competing and simultaneous need to maintain

[80] From Anklam, *Net Work,* 133.

security.[81] A dark network maintains security by adhering to rules governing the nature of relationships to securely coordinate work. When properly designed, the structure of the network is a mechanism that regulates and mitigates the exposure of critical information that if disclosed, can lead to network illumination. Illumination can have potentially fatal consequences for the dark network. Thus, we identify two dimensions to understand dark networks: the level of hostility in the external environment and the requirement for secure coordination of work.

a. External Dimension: Hostility of the Environment

The hostility of the environment affects several characteristics of the network's configuration. The legal status of a network can be directly correlated with the risk of reprisal for the network's purpose and/or activities. When opposition entities have the will and capacity to counter a dark network's illegal actions, the operational risk increases. [82] Hostility directly affects the network's dimensions related to the nature of relationships, attribution of activities, coordination of work, and the nature of governance (Figure 9). The mix of possible network characteristics depends on the network's purpose and its task environment.

[81] G. H. McCormick and G. Owen, "Security and Coordination in a Clandestine Organization," *Mathematical and Computer Modeling*, no. 31 (2000): 175-192.

[82] Doctrinal definitions for permissive, uncertain, and hostile operational environments are available at Department of Defense, *Department of Defense Dictionary of Military and Associated Terms*, April 2010, http://www.dtic.mil/doctrine/dod_dictionary/ (accessed October 26, 2010).

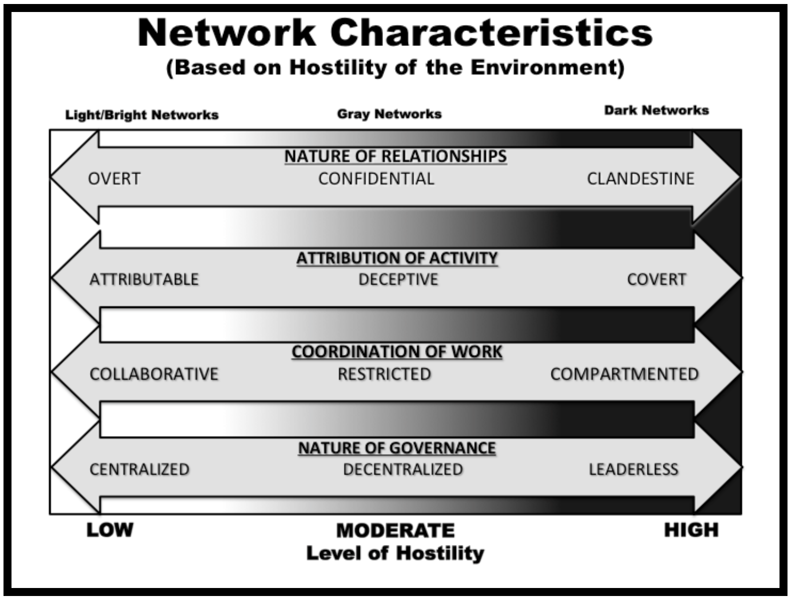


Figure 9. Network Characteristics Based on Hostility

(1) Low-Hostility Environment. A low-hostility environment is typically the domain of light/bright networks because of the licit nature of their activities. They operate in a low-risk environment that requires minimal security measures to protect against hostility. Relationships can be overt in nature; activity can be fully attributable to the network; coordination of work can maximize collaboration; and the network has the option to adopt a centralized form of governance. The low-hostility environment favors collaboration and connectivity, but is susceptible to penetration by dark network actors.

(2) Moderate-Hostility Environment. A moderate-hostility environment is typically the domain of gray networks as described earlier in chapter I. It is the domain that alerts us to the first manifestation of clandestine and covert behavior. Gray network operate in a moderate-hostility environment that requires moderate security measures. Relationships can be confidential in nature, but attribution of activity tends to be deceptive in nature. While there may be an outward appearance of legality, this is often a false front to cover illegal activity and intent. The coordination of work becomes restrictive in nature to

prevent compromise of the dark network's true intent to unvetted-unwitting members of the gray network. To offset the need for security, the networks may employ a decentralized form of governance to accomplish activities and prevent compromise. The uncertain environment represents a careful balance of security and capacity.

(3) High-Hostility Environment. A high-hostility environment is typically the domain of dark networks because of their requirements for clandestine and covert behavior. Networks operate in a high-risk environment that requires strict security measures to protect against high hostility. Relationships are usually clandestine in nature and activity is covert in nature until the act is claimed by the directional component through strategic communications. The coordination of work becomes compartmented in nature to prevent compromise of the dark network in line with the "fail-safe" principle, which will be discussed later. Information is on a strict need-to-know basis and members are constantly vetted for trustworthiness. Increased security may transform governance from a decentralized to leaderless. In "Leaderless Resistance," Louis Beam postulates that an organization is leaderless when "all individuals and groups operate independently of each other, and never report to a central headquarters or single leader for direction or instruction, as would those who belong to a typical pyramid organization."[83] A leaderless network tends to be difficult to illuminate and interdict because of the lack of ties between entities within the network united by a shared ideology, as opposed to a physical connection.

b. Internal Dimension: Secure Coordination of Work

A network's ability to sufficiently coordinate work in a secure manner relative to the hostility in the environment is typically dependent on learning tradecraft skills, or what Andrew Molnar identifies as clandestine and

[83] Louis Beam, "Leaderless Resistance," *The Seditionist*, No. 12, February 1992, http://www.louisbeam.com/leaderless.htm (accessed February 10, 2010).

covert behavior.[84] Clandestine behavior "consists of actions in which the underground member endeavors to conceal his involvement. Covert behavior attempts to conceal and cover the underground activities from observation."[85] Organizational practices, such as false fronts, records, and communications can all disguise operations. In essence, an underground has to adjust its activities depending on the environment in which it operates – this is the necessity for the secure coordination of work.

Operating in a hostile environment is inherently inefficient. Bell found that a hostile environment creates obstacles for communication between various levels of coordination, but the coordination is necessary for efficiency.[86] An "inverse ratio exists between secrecy and efficiency; absolute secrecy guarantees that nothing works properly."[87] The requirement for secrecy complicates all aspects of operation, especially in the area of command and control. Additionally, "the revolutionary ecosphere assures survival at the cost of competency."[88] The fact that most rebels want to someday assume the status of the state, most insurgents do not have the incentive to truly learn the craft of being in the underground that will create vulnerabilities in the network.

Underground organizations are dark networks and have the following characteristics: their goals are often perceived as illegal by the governmental entities they seek to overthrow; their activities are generally both legal and illegal; their members usually play legal roles within the society, with their underground membership concealed. Undergrounds, licit or illicit, must

[84] Tradecraft is the application of various techniques can be employed to achieve secrecy. See Christopher Felix, *A Short Course in the Secret War* (New York: Madison Books, 2001), 54. and Arthur S. Hulnick and Daniel W. Mattasusch, "Ethics and Morality in U.S. Secret Intelligence," in *Ethics of Spying: A Reader for the Intelligence Professional*, ed. Jan Goldman, 520-521 (Lanham: Scarecrow Press, 2006).

[85] Molnar, Tinker, and LeNoir, "Underground Organization within Insurgency," 17–35.

[86] J. Bowyer Bell, "Aspects of the Dragonworld: Covert communications and Rebel Ecosystem," *International Journal of Intelligence and Counterintelligence*, 3, no 1 (1990), 17–18.

[87] Bell, "Aspects of the Dragonworld: 15–43, 17.

[88] Bell, "Aspects of the Dragonworld: 15–43, 18.

always preserve their clandestine nature for survival. Although Molnar's study focused on underground organizations in insurgencies and revolutions from a hierarchal perspective, the characteristics are applicable to the study of dark networks when viewing his findings through the network lens. The requirement for self-preservation while accomplishing a goal in the face of environmental hostility lends itself to varied dark network configurations based on the network's goals and environmental conditions.

(1) Relationships. Theories and concepts related to relationships in light/bright networks are applicable to dark networks, but take on a higher priority to provide secrecy and prevent network illumination and interdiction. The requirement for secure coordination of work drives clandestine and covert behavior to hide illicit operations and keep the network invisible. Molnar found that human inadequacy presents the most danger in clandestine operations and one of the most critical areas of underground work is teaching members to maintain silence – unguarded conversation leads to compromise of the clandestine organization.[89] Strict rules governing communication and operational security measures give members direction and provide a set of techniques to maintain security. Parallel secure communication, operational, intelligence, and support channels are established in a manner that follow a "fail-safe" principal so that if one element fails or is compromised, the consequences to the network will be minimal.[90]

From a relational standpoint, a dark network can be considered a closed, invitation-only group that operates in an environment that is inherently inefficient and relies on trust, weak ties, and structural holes to maintain secrecy. Potential and existing members of the network must adhere to strict rules of clandestine and covert behavior and live in a state of perpetual

[89] Andrew R. Molnar, Jerry M. Tinker and John D. LeNoir, "Chapter 5: Clandestine and Covert Behavior," in *Human Factors Considerations of Undergrounds in Insurgencies*, 101–108 (Washington, D.C.: Special Operations Research Office, 1965), 105.

[90] Andrew R. Molnar, William A. Lybrand, Lorna Hahn, James L. Kirkman and Peter B. Riddleberger, *Undergrounds in Insurgent, Revolutionary, and Resistance Warfare* (Washington, D.C.: Special Operations Research Office, 1963), 54–55.

operational testing to vet loyalty and validate trustworthiness for greater access to network secrets.[91] Strong ties between actors illuminates the network and makes it vulnerable to interdiction. Conversely, weak ties and structural holes create compartmentalization and reduce the chance of compromise. As we will discuss next, the proper structure of a dark network, along with deliberate shaping of relational ties, optimizes secure coordination of work to prevent compromise and achieve the network's purpose.

(2) Structure. Raab and Milward state that networks are "coordination devices used for the benefit of the people."[92] However, further study highlights that these light/bright networks, used for benefit, have parallels with "networks and actors that pursue criminal ends."[93] They must adopt a flexible structure to enable them to react quickly to changing pressures from external entities and hostility in the environment in order to survive. Typically, dark networks tend to revert to physical force and coercion to achieve their goals.[94] Because of this necessity to protect their organizational structure and remain secret and control its members, dark networks must devote resources to enable the network's capacity for secure coordination of work. Next, we will examine how dark networks configure themselves to enable secure coordination of work by employing structural security measures.

(a) Security Measures. Reflecting on the basic network structures presented by Arquilla and Ronfeldt, a dark network incorporates additional mechanisms in order to fit the environment in which it

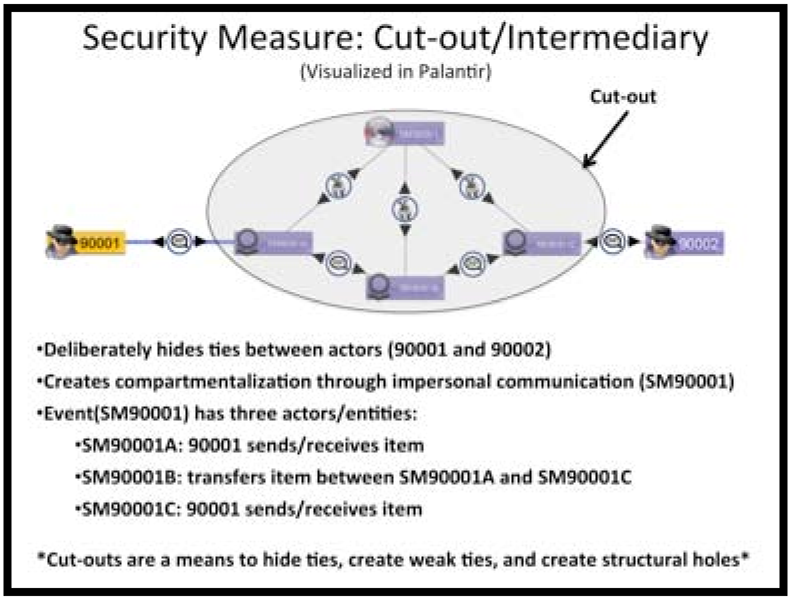
[91] Validation of loyalty, trustworthyness, and adherence to rules of clandestine and covert behavior is a constant process, which is detailed in Molnar, Tinker, and LeNoir, "Clandestine and Covert Behavior."

[92] H. Brinton Milward and Joerg Raab, "Dark Networks as Problems Revisited: Adaptation and Transformation of Islamic Terror Organizations since 9/11," *University of Southern California*, September 29, 2005, http://www.usc.edu/schools/sppd/private/documents/bedrosian/dark_networks.pdf (accessed August 4, 2010), 6–7.

[93] Milward and Raab, "Dark Networks as Problems Revisited," 7.

[94] Ibid.,7. Milward and Raab present four main propositions to guide further research on the subject of dark networks. The preceding information summarizes Proposition 1 and Proposition 4

operates. One such security mechanism is a cut-out, or intermediary. A cut-out can be a person or an event that acts as an intermediary between two actors or between two events creating a channel for clandestine impersonal communications (Figure 10).[95] Cut-outs can hide network relationships from analysts using social networking software by creating weak ties and structural holes that affect network measures scores which can inhibit identification of key players in the network.



Security Measure: Cut-out/Intermediary

(Visualized in Palantir)

- •Deliberately hides ties between actors (90001 and 90002)
- •Creates compartmentalization through impersonal communication (SM90001)
- •Event(SM90001) has three actors/entities:
  - •SM90001A: 90001 sends/receives item
  - •SM90001B: transfers item between SM90001A and SM90001C
  - •SM90001C: 90001 sends/receives item

Cut-outs are a means to hide ties, create weak ties, and create structural holes

Figure 10. Illustration of Cut-out/Intermediary Visualized in Palantir

A cut-out is an additional security measure that augments the basic network structures as a means to conduct secure coordination of work within the network (Figure 11).

[95] Christopher Felix, *A Short Course in the Secret War,* New York: Madison Books, 2001, 41.

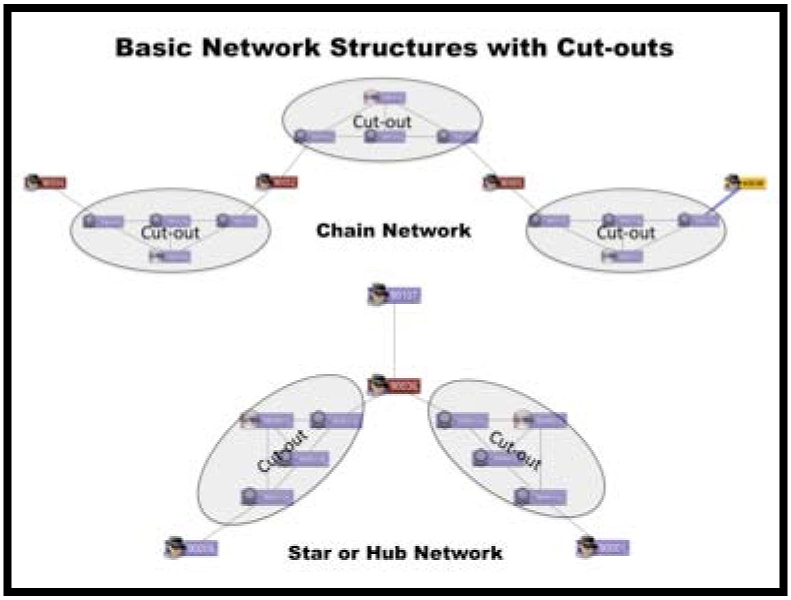


Figure 11. Basic Network Structures with Cut-outs[96]

(b) Fail-safe structures. In his study of insurgent of underground networks, Andrew Molnar found that the cellular structure and compartmentalization of information provided fail-safes that provided security and allowed the insurgency to achieve its purpose in the face of hostility.[97] The foundational construct of the underground insurgent network is the operational cell. The operational cell is composed of a leader and a few cell members operating directly as a unit. They collect money, distribute propaganda and carry on the necessary political functions of an underground. The intelligence cell usually conducts the most sensitive missions. This cell is unique in that the cell leader seldom comes into direct contact with the members of the cell and the members are rarely in contact with each other. The main characteristic of this cell is the high degree of compartmentalization and its use of indirect communication. The auxiliary cell is commonly found in front groups or in sympathizers' organizations. The auxiliary cell contains an underground cell leader, assistant cell leaders, and members. The auxiliary cell differs structurally

[96] After Molnar, Tinker, and LeNoir, "Underground Organization within Insurgency."

[97] Molnar, Tinker, and LeNoir, "Underground Organization within Insurgency."

from the operational cell in that it is normally larger in size, has an intermediate level of supervision, and has little or no compartmentalization.[98]

(i) Parallel Workflow. *Parallel workflow* is frequently set up to support a primary cell. These cells are often arranged as an alternate or redundant mechanism in case the primary cell is compromised. This not only offers protection, but is also a means of redundancy within the network. An operational branch leader could direct multiple operational cells to conduct simultaneous operations against the same target, while each cell is unwitting of the other cells existence (Figure 12). Likewise, working through a series of cut-outs, an intelligence branch leader could direct multiple intelligence cell members to gather information on the same target, or each other (Figure 13).

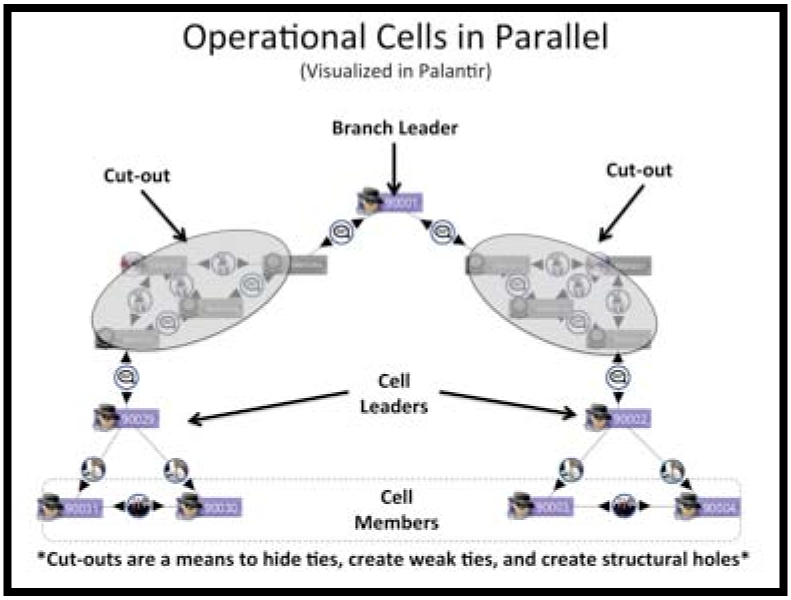

Operational Cells in Parallel
(Visualized in Palantir)
Branch Leader
Cut-out
Cut-out
Cell
Leaders
Cell
Members
Cut-outs are a means to hide ties, create weak ties, and create structural holes

Figure 12. Operational Cells in Parallel Visualized in Palantir.[99]

[98] Molnar, Tinker, and LeNoir, “Underground Organization within Insurgency,” 20–21.

[99] After Molnar, Tinker, and LeNoir, "Underground Organization within Insurgency."

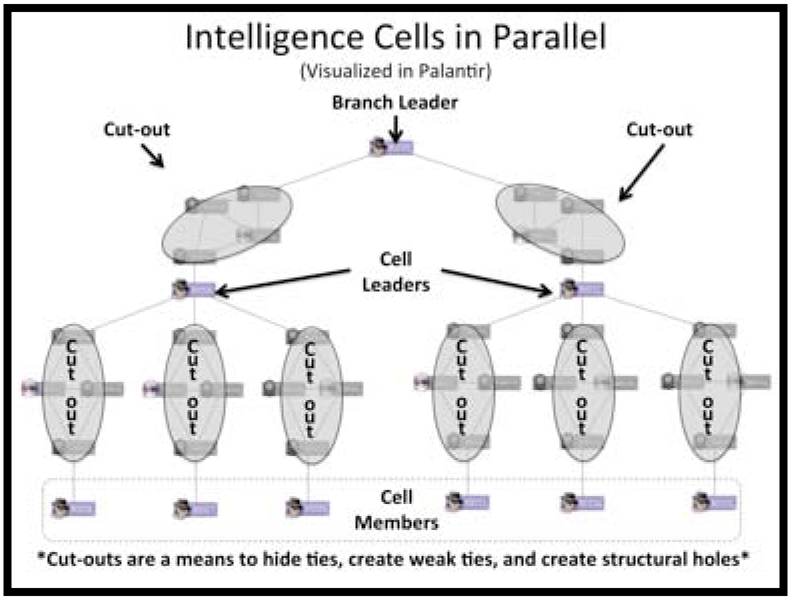


Figure 13. Intelligence Cells in Parallel Visualized in Palantir.[100]

(ii) Serial Workflow. Serial workflow is a form of sequential interdependence commonly found in supply chain networks that relies on the exchange of resources in a manner where one element's output is passed on to become the input of another element's process.[101] *Cells in Series* can be considered the illicit supply chain to the dark network. They are typically developed to carry out functions such as the manufacture of weapons, supply, escape and evasion, propaganda, and printing of newspapers (Figure 14). The nature of serial workflow requires strict adherence to clandestine and covert behavior throughout the supply chain to avoid illumination and interdiction by opposition security elements. To ensure redundancy and resilience, branch leaders may establish multiple serial workflow chains in parallel depending on the environment.

[100] After Molnar, Tinker, and LeNoir, "Underground Organization within Insurgency."

[101] See Stephen P. Borgatti and Xun Li, "On Social Network Analysis in a Supply Chain Context," *Journal of Supply Chain Management* 45, no. 2 (2009): 5-22 and Daft, *Essentials of Organization Theory and Design*.

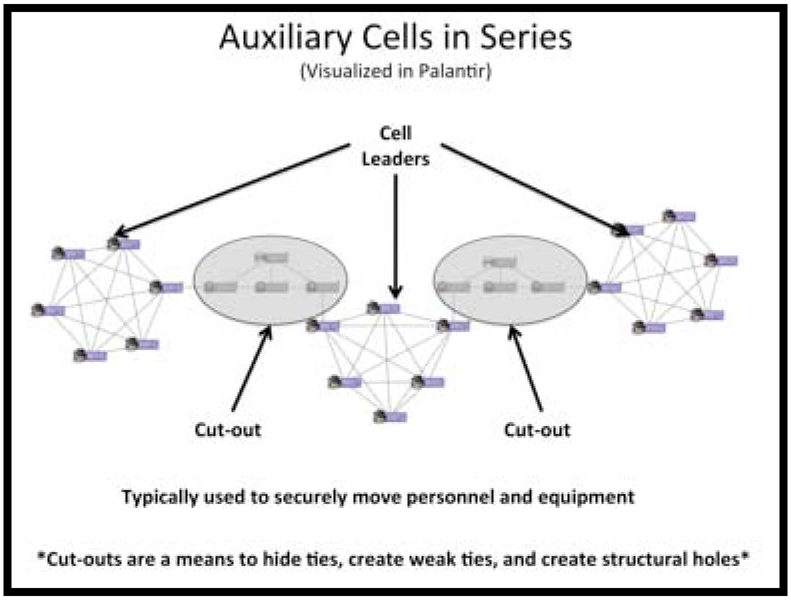

Auxiliary Cells in Series
(Visualized in Palantir)
Cell Leaders
Cut-out
Cut-out
Typically used to securely move personnel and equipment
Cut-outs are a means to hide ties, create weak ties, and create structural holes

Figure 14. Auxiliary Cells in Series Visualized in Palantir.[102]

D. SHORTFALLS IN THE LITERATURE

There is a negligible body of work on the concept of dark network design. We found the works of Marc Sageman and Derek Jones to be the most relevant current bodies of work that provide a conceptual framework for designing dark networks.

In *Understanding Terror Networks*, Sageman highlights the role that social networks play to build operational capacity for the global Salafi jihad.[103] The Salafists rely on their robust networks of trust-based relationships that provide a level embeddedness throughout the Muslim world. This embeddedness in diaspora communities provides a base of ideological and material support for the jihad. To avoid illumination and interdiction, Salafists adopt clandestine and covert behavior and leverage technology, such as mobile phones and the internet, to coordinate work in a decentralize manner through impersonal communication. While Sageman's work lends insight on how the dark networks

[102] After Molnar, Tinker, and LeNoir, "Underground Organization within Insurgency."

[103] Sageman, *Understanding Terror Networks*.

of the global Salafi jihad coordinate work in a hostile environment, he does not provide a design framework for why the networks adopt a particular configuration or implement certain security measures.

From a dark network design standpoint, the most applicable body of work we find comes from United States Army Special Forces Major Derek Jones, in his monograph: *Understanding the Form, Function and Logic of Clandestine Cellular Networks*.[104] In this work, Jones presents that the long-term survival of clandestine cellular networks and organizations relies on the principles of clandestine cellular networks. His first principle is compartmentalization. By reducing the number of people who have operational knowledge, the organization creates a virtual wall against counterinsurgent forces. Second, resilience allows the networks to survive counter-network operations and reconnect the network around nodes that have been eliminated. Third, the use of proper tradecraft allows for a low-signature, which minimizes the profile of organizational communications, movement, internetwork interaction and operations. The fourth principle is purposeful growth; the clandestine recruiting of personnel based on the purpose of the network. Fifth, operational risk addresses the paradox of the need of the network to conduct operations to maintain and build relevance versus the risk to long-term survival of the network posed by those same actions. The final principle is the idea of organizational learning: The fundamental need of a network or organization to learn and adapt to changing environmental and situational conditions. These concepts demonstrate the inherent complexity of networks.[105]

In the literature we have reviewed, a multitude of literature states that dark networks come in a variety of forms and shapes and that they must be flexible in

[104] Derek Jones, *Understanding the Form, Function, and Logic of Clandestine Cellular Networks,* (Fort Leavenworth, KS: US Army School of Advanced Military Studies, 2009).

[105] Note: the authors acknowledge that Jones' study is mainly focused on clandestine cellular networks that are one form of a dark network as defined by our study. Jones' design concepts of clandestine cellular networks can be reasonably applied to the dark network design challenges discussed in theory here.

order to effectively react to the changes in their environment, yet we found no discussion of alternative designs for dark networks.[106] Furthermore, we have not found any literature on what drives networks, especially dark ones, to adopt a particular configuration or basic structure. Although Jones provides principles for clandestine networks to follow in order to survive, neither he, nor anyone else provides a framework a for dark network design to ensure adherence to his principles of clandestine networks.

E. CONCLUSION

This chapter reviewed current bodies of knowledge pertaining to organization design and network research and found that dark networks share similar characteristics as light/bright networks, but have additional design challenges related to network relationships and structure that they must address to operate in a hostile environment. In the face of hostility, dark networks must buffer environmental hostility and coordinate work in a secure manner to produce output. Failure to design themselves to overcome those challenges may not only prohibit the network to achieve its goals, but sets the condition for catastrophic collapse of the network with fatal consequences.

Legality determines hostility that subsequently drives the need for clandestine and covert behavior. This behavior requires strict adherence to principals and techniques designed to conduct illegal activity in a secure manner in order to prevent illumination and interdiction of the dark network. Dark networks must configure themselves based on a “fail-safe” principle that controls the coordination of work in a secure manner through the deliberate manipulation of the nature of the networks relationships and structure to prevent compromise while operationalizing their purpose. Dark network design determines the optimum configuration for the task environment. In the next chapter, we will present our theory of dark network design in detail.

[106] Milward and Raab, "Dark Networks as Problems Revisited," 7, and Jones, “Form, Function, and Logic of Clandestine Networks.”

III. THEORY OF DARK NETWORK DESIGN

A. INTRODUCTION

Chapter II reviewed current literature on organizations and networks. The purpose of this chapter is to present out theory of dark network design. Current theories on dark networks do not address what determines their configuration in an effort to operationalize their network purpose. We submit that dark networks have natural configurations and that these configurations differ according to the network's purpose and design state. Although no two networks are exactly the same, we submit dark networks have similar basic components that are configured to produce output through coordinated work to achieve a purpose. First, we will review our two dimensions of dark network design: relative hostility of the environment and the requirement for the secure coordination of work. Next, we describe the four typological configurations of dark networks: Opportunistic-Mechanical, Selective-Technical, Restrictive-Organic, and Surgical-Ad Hoc. We identify and define the three fundamental components of dark networks: directional- responsible for developing and framing the network's purpose; operational- responsible for conducting decisive action to achieve the purpose; and supportive- responsible for enabling decisive action to achieve the purpose. To produce output, dark networks must overcome two critical design challenges and configure their components to buffer hostility and coordinate work. They do this by adhering to what we identify as the principles of dark network design: security, agility, resilience, direction setting, control, and capacity. Finally, we introduce our dark network system model that illustrates how a dark network coordinates work in a hostile environment to produce output and achieve its purpose.

B. DIMENSIONS OF DARK NETWORK DESIGN

1. External Dimension: Hostility of the Environment

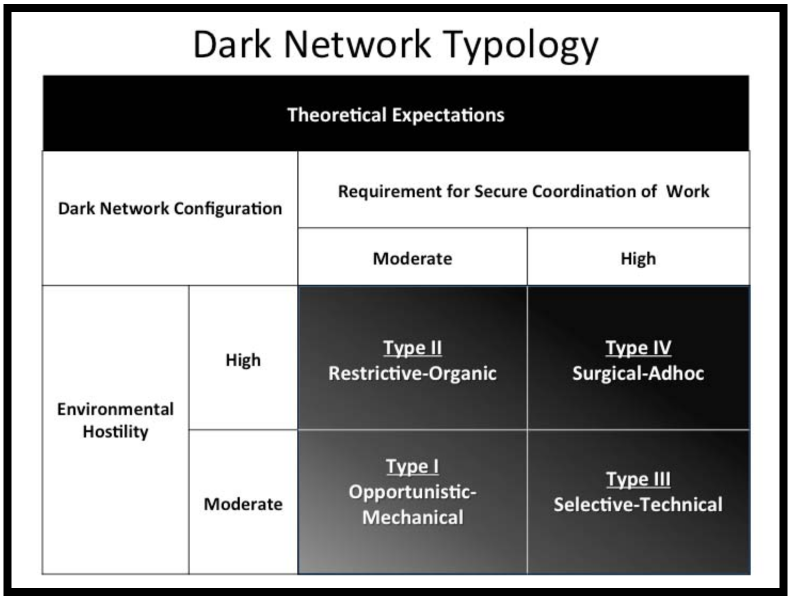
Hostility in the environment is the relationship between the dark network and its environment where opposition entities (state or non-state actors) have the will and capacity to counter the intended purpose of the dark network using lethal and non-lethal means.

2. Internal Dimension: Secure Coordination of Work

The requirement for secure coordination of work is the dark network's need and desire to commit resources to purposely create an efficient state of coordination of work in order to achieve objectives and prevent destruction.

C. DARK NETWORK TYPOLOGY

The two design dimensions, the hostility of the environmental hostility and the network's requirement for secure coordination of work, yield four pure-form design states four typological dark network configurations (Figure 15). We refer to these as design states and typological configurations as: Type-I: Opportunistic-Mechanical; Type-II: Restrictive-Organic:; Type-III; Selective-Technical; and Type-IV: Surgical-Ad Hoc.



Dark Network Typology

Theoretical Expectations			
Dark Network Configuration		Requirement for Secure Coordination of Work	
		Moderate	High
Environmental Hostility	High	Type II Restrictive-Organic	Type IV Surgical-Adhoc
	Moderate	Type I Opportunistic-Mechanical	Type III Selective-Technical

Figure 15. Dark Network Typology

1. Type I: Opportunistic-Mechanical

This type of dark network operates in an environment with a moderate level of hostility and has a moderate requirement for a secure coordination of work. Activity is opportunistic in nature and the network employs mechanistic governance. Organized criminal networks and paramilitary forces that operate in a selectively-overt (not covert) status are representative to this type of dark network. These networks are aware that the state can (and will) only use a limited application of force to inhibit their efforts. Examples include the Russian Solntsevskaya Brotherhood, Los Zetas in Mexico, and the transnational gang Mara Salvatrucha-13.

2. Type II: Restrictive-Organic

This type of network operates in environments a high level of hostility, but has a moderate requirement for a secure coordination of work. Activity is restrictive in nature because of the increased environmental hostility and is organic in nature to balance security and operational capacity. This type of network is one that is in a conflict with hostile opposition elements, but may have a high level of support from the community that gives it a more liberal freedom of movement in its environment. Type-II networks will typically maintain a clandestine and covert lifestyle, emerge conduct and overt act, and then return to the underground when threatened. Examples include Indonesia’s Jemmah Islamiyah (JI), the Haqqani network in Afghanistan and Pakistan, the South Florida-based anti-Castro movement Alpha 66, and the Provisional Irish Republican Army (PIRA).

3. Type III: Selective-Technical

This type of network operates in moderately hostile environments but have a high requirement for secure coordination of work. Activity is selective in nature because of the moderate environmental hostility and is generally requires specialized education or technical knowledge. These networks typically resemble a supply chain network with serial workflow. This type of network may be involved in smuggling, financing, and other supportive activities and generally operates from a sanctuary that provides freedom of movement and action in areas of higher hostility. Historical examples of this type of network include the French Resistance Allied pilot evacuation network during World War II and the global network of Hezbollah.

4. Type IV: Surgical-Ad Hoc

This type of network operates in an environment with a high level of hostility and has a high requirement for secure coordination of work. Activity is surgical in nature because of the high environmental hostility and the cells are generally multifunctional and ad hoc due to its strict adherence to clandestine and covert behavior. Small, highly compartmented cells and singletons operating in an area where they are constantly being hunted typify a surgical-ad hoc network. Historical examples of this type of dark network are the Israeli Mossad covert action network designed to assassinate the Black September terrorists and Mohammed Atta’s Hamburg network responsible for conducting the 911 attacks.

D. DARK NETWORK COMPONENTS

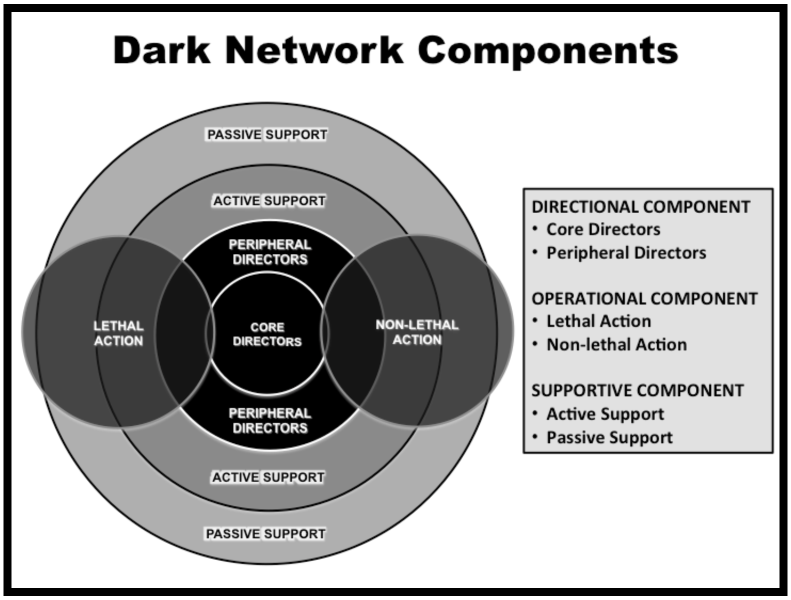


Figure 16. Dark Network Components

1. Directional Component

The directional component is responsible for developing and framing the network's purpose, what it is going to accomplish, how it is going to accomplish it, and ensures that all activities of the networks are nested in its purpose. They create the network's guiding narrative and direct its implementation. The directional component consists of the core directors and the peripheral directors.

a. Core Directors

The core directors set the strategic pace and ideology for the network. It is often removed from day to day operations, but will be considered the "face" of the network. The core directors develop and frame the network's purpose and doctrinal ideology that provides strategic direction that serves as the overarching guidance to the entire network. For example, the Tabilan's Quetta Shura, headed by Mullah Omar, serves as the core director for the Taliban network in Afghanistan and Pakistan.

b. Peripheral Directors

The peripheral directors provide direction and coordinate the work of the operational component and supportive component to produce value based on the network's purpose. In the Mintzberg sense, peripheral directors are the network's middle management, or middle line. It ensures the day-to-day operational and supportive activities nest with the network's strategic direction. The peripheral directors operationalize and direct the execution of operational and support activities based on strategic intent through specified and implied directives based on the network's purpose. The Taliban's core directors consist of the key players at the operational and tactical levels that direct the activities of the rank and file members of the operational and supportive components.

2. Operational Component

The operational component is responsible for conducting decisive action (work) to produce effects (value) that achieves the network's purpose. Decisive Action elements are the entities that achieve defined objectives required to achieve the networks objectives related to its purpose. Peripheral directors from the directional component are embedded in the operational component and assume its leadership roles and functions. Decisive action is accomplished through lethal and non-lethal action.

a. Lethal Action

Lethal action entities achieve their objectives through the decisive use, or implied use of violence using direct and indirect fire weapons that cause destructive or lethal results. These entities may be referred to as direct action elements. Lethal actions are operations or activities (work) that are typically offensive in nature (i.e. ambushes, raids, bombing, assassination, direct and indirect fires, etc.) to cause destructive effects (value) to achieve the network's purpose. Peripheral directors from the directional component are embedded in the operational component and assume its leadership roles and functions. Taliban elements that conduct attacks on the Afghan security forces and coalition partners through direct fire, indirect fire, or improvised explosives devices represent operational components that conduct lethal action.

b. Non-Lethal Action

Non-lethal action entities achieve their objectives through the decisive use of non-lethal means to execute decisive operations. Non-lethal actions are operations or activities (work) that are typically offensive in nature (i.e. cyber-attack, information operations, subversion, electronic warfare, intelligence operatives, etc.) to cause destructive effects (value) to achieve the network's purpose. Taliban information operation elements that rapidly craft and disseminate media messages designed to erode the legitimacy and degrade the operational capacity of the coalition security forces in Afghanistan and Pakistan are representative of non-lethal decisive action elements.

3. Supportive Component

The supportive component is responsible for establishing mechanisms and conducting activities (work) to provide resources (value) that enable the operational component to conduct decisive action (work) and produce effects (value) to achieve the network's purpose. The supportive component consists of active and passive supporters.

a. Active Support

Active support is full-time or part-time activity (work) by actors that are witting of the true nature of their actions (i.e. trainers, safe site keepers, financiers, transportation agents, couriers, recruiters, surveillance and early warning, supply, administrative activities, etc.) to provide resources (values) necessary to resource and enable decisive operations and the network as a whole to achieve the network's purpose. Direct support entities work in concert with decisive action elements and the peripheral directors to give them the materials they need to conduct violent or spectacular events. Indirect support elements often work on the periphery of the network structure and are in general support to the entire network. These indirect support entities typically operate in the domain of the gray networks to interface with sources of passive support. The elaborate network of witting safe house keepers, cache emplacers, intelligence agents, transportation agents, recruiters, and the supply chains that provides all forms of lethal and non-lethal materials exemplifies types of active supporters.

b. Passive Support

Passive support is witting inaction or unwitting action (work) that enables and/or provides freedom of movement or action (value) for the directional, operational, or supportive components to achieve the network's purpose. Passive supporters are generally those who are sympathetic to the network's purpose, but will not or cannot take an active role. Passive support can be financial support through putting money in jar at a local bar or simply refusing to give support to opposition forces of the dark network. Dark networks will use criteria-based networks to find sources of passive support. This shared set of attributes forms a basis of strong ties that recruiters can use to turn passive supporters to active members of the dark networks through persuasion or coercion. Passive support is the population where the dark network finds its sanctuary from hostile opposition forces. Afghans that do not outwardly reject the Taliban, or provide information to coalition security forces in order to illuminate and interdict the insurgent network, are passive supporters of the Taliban. This support may be provided willingly, or gain through coercion.

Based on our understanding of the directional, operational, and supportive components of a dark network, we are ready to examine how they work together to achieve a purpose. Next, we will present our dark network system model to illustrate how a network defines a purpose, conducts work, and produces values in a hostile environment.

E. CHALLENGES AND PRINCIPLES OF DARK NETWORK DESIGN

Dark networks must overcome inherent design challenges to conduct secure coordination of work there is an elevated level of hostility in the environment. We postulate that the two fundamental dark network design challenges are buffering external hostility and coordinating work to produce output. To overcome their design challenges, dark networks must design themselves to adhere to the principles of dark network design: security, resilience, agility, direction setting, control, and capacity. Failure to adhere to these six principals could have fatal consequences.

1. Buffering External Hostility

The first design challenge, buffering external hostility, relates insulating the network from the detrimental effects of the environment and reducing hostility. Three principles of dark network design that enable buffering are: security, agility, and resilience.

- Principle 1: Security
  Security encompasses the application technical and non-technical means and methods of clandestine and covert behavior in order to prevent illumination and interdiction of the network.
- Principle 2: Agility
  Agility entails the network's ability to adapt rapidly to changes in the environment.
- Principle 3: Resilience
  Resilience is the network's ability to react to adversity, such as interdiction by opposition elements, and return to its prior state without catastrophic network disintegration or significant reduction in operational capacity. Compartmentalization, redundancy, and decentralization contribute to the resilience of a dark network.

2. Coordinating Work to Produce Output

The second design challenge, coordinating work to produce output, is related to the development of mechanisms the enable decisive action that is necessary to achieve the network's purpose. Three principals of dark network design that are critical for coordinating work to produce output are direction setting, control, and capacity.

- Principle 4: Direction Setting

  Direction setting provides the overarching purpose for all network activities. The direction keeps members of the network engaged in their activities and focuses them on the collective goal that transcends the needs and desires of the individual actors. The strategic core and functional periphery of the directional component set the network's direction to achieve an intangible ideological purpose through decisive action that results in tangible output.
- Principle 5: Control

  Control is the coordination and synchronization of work that keeps the network focused on achieving its purpose through assignment of roles and responsibilities, evaluation of processes, and regulation of the network's resources on a continuous basis. While dark networks tend to have loose measures of control, they still require mechanisms to manage the network's resources and produce output in a secure manner that does not lead to network illumination and interdiction.
- Principle 6: Capacity

  Capacity is the development of the necessary human, physical, and virtual infrastructure to coordinate work between the directional, operational, and supportive components that enables decisive action and achieves the network's purpose.

F. DARK NETWORK SYSTEM MODEL

The dark network system model (Figure 17) provides an illustration of how the directional, operational, and supportive components of a dark network interact to produce output through secure coordination of work that is directed to a common purpose. Adhering to the principals of dark network design enables the network to produce output while buffering environmental hostility. The dark network system model summarizes the theory of dark network design.

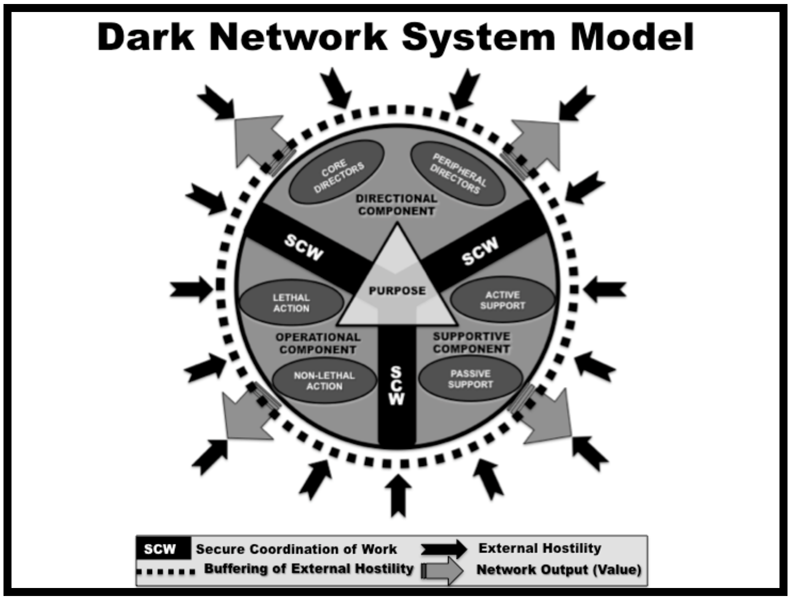


Figure 17. Dark Network System Model

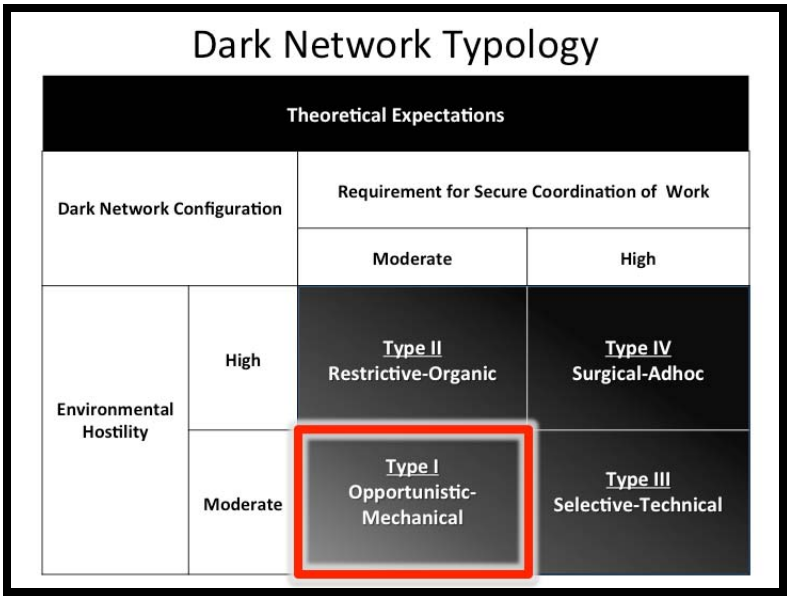
G. CONCLUSION

In this chapter, we presented out theory of dark network design. First, we showed how the level of hostility in the environment and the network's requirement for the secure coordination of work determine its design state. Next, presented four design states and typological configurations of dark networks: Type-I: Opportunistic-Mechanical; Type-II: Restrictive-Organic; Type-III; Selective-Technical; and Type-IV: Surgical-Ad Hoc. Within each design state, dark networks configure themselves by arranging three fundamental components: directional, operational, and supportive. Dark networks must configure themselves to overcome design challenges to buffer hostility and coordinate work to produce output. They do this by adhering to what we identify as the principles of dark network design: security, agility, resilience, direction setting, control, and capacity. Finally, we presented our dark network system model that illustrates how a dark network coordinates work in a hostile environment to produce output and achieve its purpose.

Looking ahead to chapters IV-VII, we apply our theory of dark network design to examine four dark networks based on our four design states. We selected our illustrative examples based on three criteria: the transnational nature of the network, the closeness of fit to the typological design state, and the availability of open source information on the network. Chapter IV examines the transnational gang Mara Salvatrucha-13 (MS-13) to illustrate a Type-I Opportunistic-Mechanical network. Chapter V examines the Provisional Irish Republican Army (PIRA) to illustrate a Type-II Restrictive-Organic network. Chapter VI examines Hezbollah in Latin America to illustrate a Type-III Selective-Technical network. Finally, Chapter VII examines the Hamburg Network that was responsible for the 9/11 attacks to illustrate a Type-IV Surgical-Ad hoc network. Our theory of dark network design will be used to analyze these examples and determine the network's configuration based on its design state and discover any vulnerability due to configurational mismatch or violation of the principals of dark network design.

IV. TYPE-I DARK NETWORK: OPPORTUNISTIC-MECHANICAL

A. INTRODUCTION



Dark Network Typology

Theoretical Expectations

Dark Network Configuration		Requirement for Secure Coordination of Work	
		Moderate	High
Environmental Hostility	High	Type II Restrictive-Organic	Type IV Surgical-Adhoc
	Moderate	Type I Opportunistic-Mechanical	Type III Selective-Technical

Figure 18. Type-I Dark Network Quadrant

The purpose of this chapter is to illustrate an example of a dark network whose design state is defined by moderate environmental hostility and a moderate requirement for secure coordination of work that yields what we call Type-I Opportunistic-Mechanical configuration. Based on our theory of dark network design, the example shows how an Opportunistic-Mechanical dark network is configured to achieve its purpose and how it is vulnerable to illumination and interdiction.

Type-I dark networks can include organized crime, gangs, mass radical movements, drug trafficking organizations, and paramilitary elements. For example, Russian Organized crime groups, such as (or the Solntsevskaya Brotherhood), conduct a variety of illicit activities that include money laundering, prostitution, human trafficking and arms dealing.[107] This group operates through dozens of small cells at home and abroad.[108] Los Zetas, a Mexican drug cartel tied to a wide range of criminal activities, such as human trafficking, kidnapping and extortion, operates in a cell-like networked structure to limit information and remain agile in their environment.[109] One report states they are well armed and operate at a higher tactical level than local authorities, which gives them freedom of movement.[110]

For our illustration of a Type-I dark network configuration, we use the transnational gang Mara Salvatrucha-13 (MS-13). Although MS-13 has degrees of variation within the network, we selected it over the others because of its transnational nature; it most closely illustrates the typological design state of a Type-I dark network; and its prominence provides a rich collection of open-source information on the dark network.

B. OVERVIEW OF MARA SALVATRUCHA-13

The transnational nature and expanding influence of MS-13 presents an increasing threat to U.S. national security and stability in the Western Hemisphere. In the early 1980s through the 1990s, over 2 million immigrants fled from civil wars that ravaged Central America and into the United States of America. Most of the immigrants fled from El Salvador and settled in the Los Angeles, California area. In the Los Angeles area alone, the Salvadoran

[107] Ramon J. Miro, “Organized Crime and Terrorist Activity in Mexico, 1999-2002”, *Library of Congress Report* (February 2003), http://www.loc.gov/rr/frd/pdf-files/OrgCrime_Mexico.pdf (accessed on November 29, 2010), 29.

[108] Ibid., 29. Also see Gretchen Peters, “Drug Trafficking in the Pacific Has a Distinct Russian Flavor,” *San Francisco Chronicle,* 30 May 2001, http://articles.sfgate.com/2001-05-30/news/17600134_1_svesda-maru-russians-largest-cocaine-seizure (accessed on November 29, 2010).

[109] United States Congress, *Weak Bilateral Law Enforcement Presence at the U.S.-Mexico Border: Territorial Integrity and Safety Issues for American Citizens*, Joint Hearing of the 109th Congress, 1st Session, November 17, 2005, (Washington D.C.: U.S. Government Printing Office, 2006), 6–7; Michael Ware, “Los Zetas called Mexico’s most dangerous drug cartel,” *CNN.com/world*, http://www.cnn.com/209/WORLD/americas/08/06/mexico.drug.cartels/index.html (accessed on November 29, 2010).

[110] United States Congress, Weak Bilateral Law Enforcement, 6–7.

population grew from 30,000 to 300,000; a vast majority of them, due to not being granted refugee or asylum status, were illegal aliens.[111] MS-13 reportedly originated in Los Angeles in the 1980s as a result of victimization of Salvadoran immigrants by local Hispanic gangs. The large number of Salvadoran immigrants banded together and formed the MS-13 gang as a means of protection.[112] Over time, the gang grew and evolved from a means of protecting the Salvadoran immigrants to participation in a variety of activities ranging from extortion to drug trafficking.[113]

As law enforcement cracked down and began deporting MS-13 members, the gang used the deportation to their advantage. First, the deportees set up MS-13 cells in their native country of El Salvador and expanded into Honduras and Guatemala. Second, the deported members found that Central America was a prime recruiting ground and began recruiting new members. These new recruits flooded into the United States to flee the law in their home country and others joined their families on the "immigrant trail," which led to the establishment of cliques (geographically defined subgroups) throughout the United States.[114] Currently, MS-13 has active operations in 42 states and the District of Columbia with 6,000-10,000 members nationwide, in addition to operations in El Salvador,

[111] Jessica M. Vaughan and Jon D. Feere, "Taking Back the Streets: ICE and Local Law Enforcement Target Immigrant Gangs," *Center for Immigration Studies Backgrounder* (October 2008), 5.

[112] Celinda Franco, "The MS-13 and 18th Street Gangs: Emerging Transnational Gang Threats?" *CRS Report for Congress*, January 22, 2010, http://opencrs.com/document/RL34233 (accessed on August 11, 2010); and Fred Burton, "Mara Salvatrucha: The New Face of Organized Crime?", http://www.stratfor.com/memberships/48568/mara_salvatrucha_new_face_organized_crime?ip_auth_redirect=1 (accessed on August 11, 2010).

[113] William J. Harness, "MS-13 Mara Salvatrucha", Conroe ISD Police Department Report (2006), http://police.conroeisd.net/Docs/MS%2013%20Gang.pdf (accessed April 11, 2010), 4.

[114] Harness, "MS-13," 4.

Honduras, and Guatemala.[115] Other reports show activity in 48 states, Washington, D.C., and Puerto Rico—the only states showing no activity are South Dakota and Vermont.[116]

According to a report from the Congressional Research Service, street gangs are characterized as a first-generation, a second-generation, or a third-generation gang.[117] A first-generation gang is a traditional, turf-oriented and localized street gang. It is relatively unsophisticated, engages in criminal activities and tends towards a loose leadership structure. A second-generation gang is more organized and tends to "assume a market rather than a turf orientation."[118] While most urban gangs fit the description of a first or second-generation gang, there is evidence that MS-13 has some characteristics of a third-generation gang. A third-generation gang is characterized as a "highly sophisticated" and "mercenary-type group[s] with goals of power or financial acquisition and a set of fully evolved political aims."[119] Although MS-13 does not appear to have fully developed into a third-generation gang nor does it have known links to terrorist groups, some researchers assert that these types of gangs and terrorist groups share similar characteristics, such as "a propensity for indiscriminate violence, intimidation [and] coercion [that] transcend[s] borders, and target[s] nation-states."[120] Currently, MS-13 is a first-generation gang with elements of—and possibly evolving into—a third-generation gang. It characterized by the "opportunistic criminal activity and inter-gang rivalry"[121] of first-generation gangs and its cells also employ tactics characteristic of third-generation gangs.

[115] From the FBI, http://www.fbi.gov/news/stories/2008/january/ms13_011408 (accessed on October 29, 2010).

[116] Vaughan and Feere, "Taking Back the Streets," 1.

[117] Franco, "The MS-13 and 18th Street Gangs," 3.

[118] John P. Sullivan, "Transnational Gangs: The Impact of Third Generation Gangs in Central America," July 1, 2008; quoted in Franco, "MS-13 and 18th Street Gangs, 4.

[119] Franco, "The MS-13 and 18th Street Gangs," 4.

[120] Sullivan, "Transnational Gangs," in Franco, "MS-13 and 18th Street Gangs," 3–4.

[121] Franco, "The MS-13 and 18th Street Gangs," 3–4.

C. TYPE-I DESIGN STATE

1. Moderate Hostility of the Environment

The Type-I design state's level of hostility in the environment can vary. The groups in this design state are already at a medium level of hostility due to their intent to commit illicit activities. Moderate hostility of the environment results when the opposition elements lack the will and/or capacity to counter the dark network. The dark network and opposition elements then reach equilibrium where the opposition accepts a certain level of illegal activity by the dark network before committing or acquiring additional assets for interdiction. Beyond MS-13, another example of this type of network may be a radicalized faction of a legal light/bright network that conducts illegal activity in support of a similar purpose. For example, protesting abortion is not illegal, but Pro-Life activists who bomb clinics or perform crimes against medical practitioners who either perform or support the performance of abortion are performing illegal acts. These individuals and groups tend not to hide their affiliation and in some cases are protected by their constitutional rights as long as they do not commit acts of violence. Once they conduct illegal activity, hostility becomes high for individual actors and the network as a whole.

This variance in environmental hostility is evident in our MS-13 example. Environmental hostility varies from clique to clique within the United States, mostly dependent upon level and frequency of crime and capability and/or priority level of local law enforcement. The hostility also varies transnationally. In El Salvador, local officials have adopted a hard-hitting approach called *Mano Dura* to combat the gang and are beginning to make it more difficult for MS-13 to carry out its operations. For this reason, MS-13 in El Salvador appears to be transitioning to a more hierarchical structure and adopting more secure measures to coordinate its activities.[122]

[122] Clare Ribando, "Gangs in Central America," *CRS Report for Congress* (May 10, 2005), http://www.fas.org/sgp/crs/row/RS22141.pdf (accessed on November 29, 2010), 3–4. Also see Vaughan and Feere, "Taking Back the Streets."

2. Moderate Requirement for Secure Coordination of Work

The moderate hostility in the environment also lends itself towards the moderate requirement for secure coordination of work to achieve the network's purpose. A Type-I configuration does not rely on a high degree of compartmentalization or clandestine communication to accomplish its tasks because it does not have to. The environment that a Type-I dark network operates, while not necessarily friendly, affords freedom of movement because the legitimate government may have neither the will, nor the capacity, to effectively combat dark network. Reduced security requirements make coordination of work less restrictive and more collaborative. The individuals and networks in this quadrant are can have meetings in the open, advertise their affiliations, and do not need to conceal their true identities.[123] Details of specific operations may be guarded, but their goals are not. In the case of MS-13, the gang does not conceal its goal of being the most violent gang in the world. It will use some measure of protection to prevent compromise of gang operations, such as using code words and/or utilizing the MS-13 alphabet in correspondence, but they do not hide the fact that they are drug traffickers, murderers, or kidnappers.

D. TYPE-I DARK NETWORK: OPPORTUNISTIC-MECHANICAL

We characterize Type-I dark networks as opportunistic and mechanical for the following reasons:

1. Opportunistic Action

The opportunistic nature of this dark network indicates a desire to make money, obtain and hold power, and follow the model of "any crime, any time" as long as it is profitable. Opportunistic action means to be involved in "a variety of criminal enterprises and is willing to commit almost any crime for monetary

[123] Gang members tend to adopt street names (pseudonyms) that become or their *nom de guerre*. Over time, gang members may only be known by their street name and create a de facto "cover" that makes illumination of the dark network problematic.

compensation."[124] For example, MS-13 is implicated in a myriad of illicit activity, such as extortion, rape, drug trafficking, human trafficking, murder, theft, assault, prostitution throughout the United States and Central America.[125]

2. Mechanical Configuration

In a Mintzberg-sense, a mechanistic network resembles the diversified configuration—also known as a divisional or matrix form of organizational structure—that is selectively decentralized at the network level, centralized and authoritarian at the clique/cell level, and relies on the standardization of outputs to coordinate work and achieve the network's purpose.[126] Networks in this quadrant primarily operate in a decentralized manner, but recognize a system of relative power and authority and adhere to a strict set of norms promulgated by the strategic core of the directional component.[127] This recognized informal influence structure provides a framework for formal authority should the dark network decide to adopt a hierarchal form of organization as the situation permits.[128]

[124] Commonwealth of Virginia Department of State Police Virginia Fusion Center, "Mara Salvatrucha 13 (MS-13) Intelligence Report," July 2008, http://info.publicintelligence.net/VFCMaraSalvatrucha.pdf (accessed on November 15, 2010), 4.

[125] List of MS-13 crimes compiled from FBI, ICE, and various law enforcement agency reports. For one source, see The Federal Bureau of Investigation (FBI), "The MS-13 Threat: A National Threat Assessment", http://www.fbi.gov/news/stories/2008/january/ms13_011408 (accessed on August 11, 2010).

[126] Mintzberg, *Mintzberg on Management*, 153–172.

[127] Michael K. Carlile, *Into the Abyss: A Personal Journey into the World of Street Gangs*, April 7, 2010, http://people.missouristate.edu/MichaelCarlie (accessed November 5, 2010).

[128] In the unconventional warfare (UW) setting, an example of this evolution is when autonomous operational cells of the insurgent underground create the condition that they defeat the state security forces and become the de facto state. The relative hostility of the environment is moderate and there is a moderate requirement for secure coordination of work. Thus, they can assume an overt presence and grow and assume the duties and responsibilities as the legitimate authority. At this stage, these elements tend to adopt a recognized uniform and become the guerrilla elements of the insurgency and adopt a hierarchal form of organization. See Mark Grdovic, "SWCS PUB 09-1: A Leader's Handbook to Unconventional Warfare," *United States Army John F. Kennedy Special Warfare Center and School*, November 2009, http://www.soc.mil/swcs/swmag/Assets/SWCS%20Publications/Leaders%20Guide%20Final.pdf and Department of the Army, "U.S. Army TRADOC G2 Handbook No.1: A Military Guide to Terrorism in the Twenty-First Century," *Air War College Conflict 21 Terrorism Studies*, August 15, 2007, http://www.au.af.mil/au/awc/awcgate/army/guidterr/guidterr.pdf.

Although networks by definition do not have a formal hierarchy, governance does exist in varying degrees throughout the network by means of an informal power structure recognized by members of the network. This informal architecture of power and authority is based on respect and is guided by strict set of rules and norms.[129]. This mechanical network does not have a single leader, but a virtual "big man" or directional nodes may emerge at various points in the network.[130] While cells within this network may have little to no communication with one another, each cell tends have central actors who are responsible for not only representing the interest of their respective cell or clique, but also maintaining the established norms of the network and achieving its purpose. In some cases, there may be more discernable structures or roles that exert greater influence based on an actor's centrality, power, or prestige in the network.[131] Reflecting on *The Advent of Netwar*, Arquilla and Ronfeldt's term "panarchy" best describes the aforementioned pseudo-hierarchy and how networks are able to selectively decentralize and standardize outputs through a strong purpose and set of established norms:[132]

> Performance over time may depend on a powerful doctrine or ideology, or at least a strong set of common interests and objectives, that spans all nodes, and to which the members subscribe in a deep way. Such a doctrine can enable them to be "all of one mind" even if they are dispersed and devoted to different tasks. It can provide an ideational, strategic, and operational centrality that allows for tactical decentralization. It can set boundaries and provide guidelines for decisions and actions so that

[129] See Mintzberg, *Mintzberg on Management*, 132–152.

[130] Dr. Anna Simons, "The Anthropology of Conflict" (lecture, Naval Postgraduate School, Monterey, CA, October 6, 2010). A "big man" is an influential individual with no formal authority. His skills, possessions, wisdom, or another trait revered in a particular society, place him in a position of elevated status or recognition.

[131] Everton, *Tracking, Destabilizing, and Disrupting Dark*), 109–125, and Carlos A. Poveda, *The Likelihood of Collaboration Between Central American Transnational Gangs and Terrorist Organizations* (Monterey: Naval Postgraduate School, 2007), 19.

[132] John Arquilla and David Ronfeldt, "RAND Monograph Reports: The Advent of Netwar," *RAND Corporation*, 1996, http://www.rand.org/pubs/monograph_reports/MR789/ (accessed November 5, 2009), 10.

> they do not have to resort to a hierarchy—'they know what they have to do.' That is why a nouveau term like panarchy may be more accurate than heterarchy.

When cliques within the network do not "do what they know they have to do," the directional elements of the network may exercise centralized authority on a selective basis in order to maintain the standards of the network. Once the crisis is resolved, the network will return to the selectively decentralized status quo. At the clique level, governance tends to be highly mechanical and authoritarian in nature based on the network's purpose and ideology. This loose construct of semi-autonomous cliques (cells) that are unified by a common purpose and an established set of norms enable the network to selectively decentralize for greater security. This arrangement provides a fail-safe that ensures the compromise of one cell will not impact the network as a whole. Likewise, the removal of a particular network cell leader does little to topple the entire network. Instead, it will allow for others to rise and assume control within the cell.

E. FUNDAMENTAL COMPONENTS

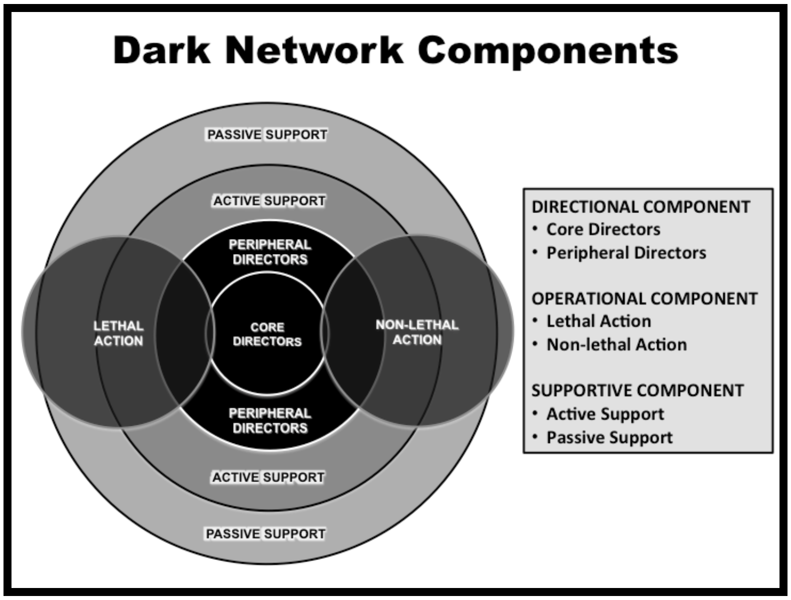


Figure 19. Illustration of Dark Network Components

1. Directional Component

MS-13 began as a local street gang, formed for protection, in the Hispanic barrios of Los Angeles and was not originally associated as a criminal organization. It existed to protect the safety of its members and members "held in high regard" served as the gang's decision makers. MS-13's purpose has evolved over time. The motto of Mara Salvatrucha is "Mata, Viola, Controla," or "Kill, Rape, Control." Despite originally forming to protect El Salvadoran immigrants in the Los Angeles area from Mexican gangs, Mara Salvatrucha now strives to become and remain the most violent and most feared gang in the world.[133] Their crimes may vary from clique to clique, depending on location and direction from local gang leaders, but the overall purpose is to be violent and make money. Members of MS-13 have been convicted of crimes ranging from murder for hire to extortion to prostitution and rape. One account in the Northern Virginia area describes an extortion ring where the gang members tax the parents of young girls for "protection money" to ensure the young girls are not raped. While operating in loose-autonomous cells with little to no visible hierarchy, this continuity of purpose is maintained through the common desire to be the most feared gang. This attitude is fueled by media reports, documentaries, and the increase of Congressional Hearings on gang violence, where MS-13 is the headline gang of record.[134]

The network's configuration of loose, autonomous cells makes it resilient. Taking out a "leader" just activates a promotion system for emergent leaders. While there may be a lull in operations, the gang is not stopped and authority remains intact while the gang member serves his/her jail time. Interdiction does not result in catastrophic network disruption and deportation does not work. In

[133] *World's Most Dangerous Gang*. DVD. Produced by Andrew Tkach (2006), U.S.A. and Canada: Warner Home Video, 2006.

[134] Vaughan and Feere, 8. Also see "MS-13 and Counting: Gang Activity in Northern Virginia", Hearing before the Committee on Government Reform – House of Representatives, 109th Congress, 2nd Session, July 14, 2006, serial no. 109-174 and September 6, 2006, serial no. 109–182. Available at https://www.house.gov/reform.

one case, a MS-13 member was arrested in Suffolk County, Virginia, and New York on drug charges, was deported, and immediately returned to the United States and was subsequently arrested in Yuma, Arizona.[135] Similarly, another MS-13 member arrested in Santa Cruz, California in June 2010 had been deported three times in the previous eight years.[136] Further, deportation of undocumented MS-13 gang members has resulted in a networked, criminal diaspora throughout the Americas.[137] Arresting members of the directional component does not remove them from the network on a permanent basis.

MS-13 is organized into geographically defined subgroups, or "cliques", operating as loose, autonomous cells with the largest active concentrations in Los Angeles, CA, Washington D.C./Northern Virginia and New York City. It is widely believed that Los Angeles gang members have an elevated status among their MS-13 counterparts across the country.[138] In each setting, the gang's directional component *morphs* to fit the environment. While machete attacks might occur on the East Coast, they are rare on the West Coast. While car thefts and drug trafficking might be big in North Carolina, gang-on-gang violence predominates in Virginia. The decentralized nature of MS-13—with no clear hierarchy or structure at the network level—makes interdicting the gang as a transnational entity particularly challenging for law enforcement authorities. Law enforcement officials admit, "Taking out the heart of the leadership is very hard if there is no definitive leadership."[139] Unlike the hierarchal and formal structure of

[135] James Gilbert, "Yuma Border Patrol Agents Arrest MS-13 Gang Member," *Yuma Sun,* retrieved from http://www.yumasun.com/common/printer/view.php?db=yumasun&id=49993 (accessed on October 13, 2010).

[136] KSBW News "Suspected MS-13 Gang Leader Arrested in Santa Cruz," http://www.ksbw.com/news/23772715/detail.html (accessed December 1, 2010).

[137] John P. Sullivan and Samuel Logan, "MS-13 Leadership: Networks of Influence", *The Counter Terrorist,* August/September 2010, http://digital.ipprintservices.com/display_article.php?id=428186 (accessed on November 9, 2010).

[138] The Federal Bureau of Investigation (FBI), "The MS-13 Threat: A National Threat Assessment", retrieved from http://www.fbi.gov/news/stories/2008/january/ms13_011408 (accessed on August 11, 2010).

[139] William J. Harness, "MS-13 Mara Salvatrucha", Conroe ISD Police Department Report (2006), http://police.conroeisd.net/Docs/MS%2013%20Gang.pdf (accessed on April 11, 2010), 4.

MS-13 in El Salvador, there is no clear indication of a formal command structure within the U.S. at the network level.[140] Despite this, there is evidence that smaller, junior cliques take cues from larger, more senior cliques—namely Los Angeles—and "whenever a more senior clique declares another gang as an enemy, all junior cliques follow suit and make the same declaration."[141] Some law enforcement agencies report increasing indications of contact and synchronization among the larger MS-13 chapters in Los Angeles, Washington D.C, Northern Virginia, New York City. This could be signaling an attempt to build a "national command structure" due to the expanding size of the gang and increased need for centralized control[142]

At the clique level, the close geographic distribution of its members and permits a centralized, almost totalitarian form of governance. For example, cliques in Los Angeles have established an internal organizational structure with assigned functional roles and responsibilities. The U.S. Department of Justice states, "Several Los Angeles cliques have adopted a military-type organizational structure, appointing captains, lieutenants, and soldiers."[143] These larger chapters currently form the strategic leadership of MS-13, providing the overall purpose and direction of the gang. While there is no clear indication of direct control over the cliques, there is evidence of an "approval process in some kind of hierarchy beyond the clique" including cases where MS-13 leaders have sent

[140] Jessica M. Vaughan and Jon D. Feere, "Taking Back the Streets: ICE and Local Law Enforcement Target Immigrant Gangs," *Center for Immigration Studies Backgrounder* (October 2008), 9.

[141] Commonwealth of Virginia Department of State Police Virginia Fusion Center, "Mara Salvatrucha 13 (MS-13) Intelligence Report," July 2008, http://info.publicintelligence.net/VFCMaraSalvatrucha.pdf (accessed on November 15, 2010), 5.

[142] Vaughan and Feere (2008), 9. Quoting Mr. Paul McNulty, the former U.S. Attorney for the Eastern District of Virginia.

[143] United States Department of Justice, "Mara Salvatrucha," *Drugs and Crime Gang Profile*, November 2002, http://webzoom.freewebs.com/swnmia/mara.pdf (accessed on November 15, 2010).

"emissaries" to give direction to underperforming or "quieter" cliques.[144] John P. Sullivan and Samuel Logan best describe the MS-13 panarchy through what they call the "hierarchy of respect":[145]

> In operational terms, the "hierarchy of respect" is expressed through a web of social relationships within individual cliques and social/business relationships between cliques. At the clique level, leadership is distributed. There are two primary leaders, the "first word" (*primera palabra*) and the "second word" (*segunda palabra*) who operate something like a commander and an executive officer in military settings. The *segunda palabra* from large, powerful cliques often exerts influence over smaller or subordinate cliques. In many facets, this leadership is neo-feudal, where leadership is determined by fealty to a leader who collects taxes and the support of warriors and in turn offers protection.

The loose-autonomous nature of the cells within the United States differs from the cliques in Central America. In El Salvador, the cliques are well organized and follow a formal command hierarchy.[146] We posit that this variation in organizational configuration between the U.S., that adopts a networked form of organization, and foreign elements of MS-13, that adopts a more formal form of organization, is a result of differing conditions of the external environment and the age of the cliques.

2. Operational Component

Within its operational component, MS-13 utilizes brutal violence (lethal decisive action), intimidation, and coercion (non-lethal decisive action) on rival gangs, the population, police, government officials, and on its own members. As previously mentioned in the *Directional Component* section, each separate clique conducts the operations they feel fit their environment in order to make money and exert influence and control. If the environment allows for drug running and prostitution rings in Chicago, then that clique will exploit that opportunity. As the

[144] Vaughan and Feere, "Taking Back the Streets," 9–10.

[145] Sullivan and Logan, "MS-13 Leadership,"

[146] Commonwealth of Virginia Department of State Police Virginia Fusion Center, "Mara Salvatrucha 13 (MS-13) Intelligence Report," 5.

environment begins to turn more hostile, law enforcement cracking down on the drug trade for example, then the clique may move its area of operations or transition to another activity. The same holds true for adjusting the use of lethal and non-lethal decisive action. An MS-13 clique in Maryland was instructed by another, more established, local clique to do more killing by increasing their "output" to kill two rival gang members every 15 days. Realizing this would result in a crackdown by local police, the increase was overruled and the clique opted instead to increase its coercion and intimidation tactics.[147]

MS-13 is agile and is not as concerned with security in the sense that it does not hide its existence from law enforcement. In most regions, Law Enforcement Agencies (LEAs) are unable to respond effectively to the violence of the MS-13 cliques. MS-13 prefers quantity (killing rival gang members, controlling local drug industry or prostitution ring, etc) to security. Being arrested and either jailed or deported does not affect their "productivity." In regions where more security measures are required due to an increase in law enforcement capabilities, MS-13 has responded by using members who do not have visible tattoos and moving meetings to less obvious locations. In one area, the gang formed a soccer team so that they had a reason to meet in the open. They also employ very basic security measures to protect day-to-day operations and knowledge from outsiders. For example, MS-13 has its own slang as well as its own alphabet.[148] This security is not only performed outside the gang, it is also verified inside. It is not unheard of for a "credit check", which is a background to ascertain someone's standing within the MS-13 gang, to verify security within.

Depending on current environment, the gang adapts its level of violence or crime of choice. In some cases, operations are moved all together (but not

[147] Testimony of Noe Cruz, in U.S. vs. Edgar Alberto Ayala and Oscar Ramos Velazques, quoted in Sam Logan and Ashley Morse, "MS-13 Organization and U.S. Response," February 2007, www.samuellogan.com (accessed on October 31, 2010).

[148] Commonwealth of Virginia Department of State Police Virginia Fusion Center, "Mara Salvatrucha 13 (MS-13) Intelligence Report," 17-18. For example, the phrases such as "collecting rent" and "touch-up" mean "extortion money" and "non-lethal assault" respectively.

stopped): "some attribute the rise in gang activity in Maryland to the success of the Regional Gang Task Force here in Virginia…instead of reducing gang activity, we are just spreading it around."[149] Agility of MS-13 is also enabled by a variety of other circumstances:[150]

> The fluidity of our borders, insufficient immigration enforcement tools, a lack of social programs that promote youth development, the persistence of poverty, and a limited regional approach to law enforcement create the perfect storm for violent gangs to thrive.

As previously stated, MS-13 exerts control on both the population and the gang itself. Enforcement is brutal. We need to look no further than the gang's motto to know their methods of control include coercion and intimidation. Coercion and intimidation is used on both the population and the gang members themselves.

3. Supportive Component

Law enforcement agencies incorrectly assume that Mara Salvatrucha's lack of a clear, formal hierarchy and its utilization of decentralized control equates to a lack of capacity. The network derives its support capacity through its members' desire to be affiliated with the gang and provides a wide base of active and passive support for the gang. Support is generated through coercion and intimidation, which is typically tied to the use, or implied use of lethal force.

Constant recruitment and a surprising level of sophistication of its supportive component provide MS-13 the infrastructure that is necessary to achieve its purpose. With an estimated 10,000 "hard-core" members in the U.S. alone, officials indicate that MS-13 is the "fastest-growing and most violent street gang in the United States."[151] The Center for Immigration Studies states, "Since its origin, MS-13 has evolved from a single turf gang into a networked

[149] Congressman C.A. "Dutch" Ruppersberger, in a statement made on his website, available at http://dutch.house.gov/2006/07/07-14-06-MS13Gang.shtml (accessed on November 6, 2010).

[150] Ibid.

[151] Vaughan and Feere, "Taking Back the Streets," 4.

organization comprised of individual ‘cliques’ that interact on the basis of social networks, influence, and opportunity”.[152] Appealing to both poverty-ridden regions and at-risk youth, membership MS-13 offers both a job and a family. “The Maras offer a code, a family to members, many of whom come from broken homes or the streets.”[153] The appeal of MS-13 generates its base of active and passive support.

There are many indications of both active and passive support for MS-13. Active support comes from families who were part of the original gang that formed in the 1980s, some of them raising their children and grandchildren to become MS-13 gang members, and employers who knowingly employ workers with known MS-13 ties.[154] Most gangsters do not make enough money to live the lifestyle full-time. According to a report from the Center for Immigration Studies, a town in Virginia discovered an MS-13 gang member working in an elementary school using false documents to obtain employment. It is assumed that many employers, family members and neighbors are “completely unwitting about [their] gang involvement” and even complain when arrests occur, “Everyone loves the guys during the day [for their labor] but it’s at night when they cause me [and the police] all the problems,” claimed one Virginia state trooper.[155]

A variety of people and institutions are passive support elements for the gang—sometimes unwittingly. A majority if MS-13 gang members (including those who are illegal aliens) work legitimate day jobs. The employers of these individuals are unwitting actors in the sustainment of MS-13. Additionally, the

[152] Sullivan and Logan, “MS-13 Leadership.”

[153] Jeremy McDermott, “Youths Flock to Massive El Salvadoran Gang that is their Only Chance of a ‘Job’,” *The Scotsman,* sec. International, April 13, 2004, http://thescotsman.scotsman/international.cfm?id=416482004&format=print (accessed April 2, 2010).

[154] *World’s Most Dangerous Gang*. DVD. Produced by Andrew Tkach (2006), U.S.A. and Canada: Warner Home Video, 2006.

[155] Vaughan and Feere, 8. Also see “MS-13 and Counting: Gang Activity in Northern Virginia”, Hearing before the Committee on Government Reform – House of Representatives, 109th Congress, 2nd Session, July 14, 2006, serial no. 109–174.

gang also uses the U.S. immigration and deportation processes to their advantage. The 1996 Illegal Immigration Reform and Immigrant Responsibility Act (IIRIRA) enabled Los Angeles law enforcement to crack down on MS-13 activity. The result was increased deportations. In some reports nearly 20,000 Central American criminals were deported from the United States from 2000 to 2004. Once these criminals returned to El Salvador, they discovered "fertile ground for recruitment" due to severe poverty, lack of economic opportunity, and limited capabilities of local law enforcement.[156] The large number of deported criminals extradited to El Salvador overwhelmed a government already focused on restoring order for thousands of refugees returning after the signing of the Chapultapec Accords.[157] While not the intention of the IIRIRA or other immigration laws, these policies enabled MS-13 to become a transnational gang. As these members were deported, either for their illegal immigrant status or for committing crimes as noncitizens, they returned to their home countries and began recruiting. This allowed gang to grow in popularity and plant roots throughout Central America. There are reports of MS-13 members being intentionally deported to gain intelligence on the new U.S. immigrations system and later disseminating their findings from prisons in Central America. The deportation process has turned into a sort of "merry-go-round" and in many cases a "taxpayer-financed visit with friends and family."[158]

The prisons in El Salvador have become "nerve centers" allowing for gang members from Los Angeles to communicate with members from cliques across the U.S. and Central America.[159] Even our own prison system has become a

[156] Vaughan and Feere, "Taking Back the Streets," 6.

[157] Embassy of El Salvador, "The Peace Accords," http://www.elsalvador.org/embajadas/eeuu/home.nsf/politics (accessed on October 23, 2010).

[158] Robert J. Lopez, Rich Connell and Chris Kraul, "Gang Uses Deportation to It's Advantage to Flourish in U.S.," *Los Angeles Times*, October 30, 2005, local edition, http://www.latimes.com/news/local/la-me-gang30oct30,0,6717943.story (accessed on October 31, 2010).

[159] Ibid.

form of passive support. Prisons offered a “finishing school” for gang members where hey learn criminal skills, later used to establish their illegal networks throughout the region[160]

To maintain control, MS-13 has its own court system. The court enforces the norms set forth by the directional component and deals with non-compliance by issuing a “green light” that sanctions the use of lethal force to deal with those who do not comply with the directives of MS-13. For example, “the failure to pay the [protection] tax results in a green light allowing any affiliated gang to kill violators in jail, prison, or on the street.”[161] This brutal enforcement mechanism allows the gang to ensure adherence to its “management vision” throughout the network. Similar control through coercion and intimidation is exercised on the local population.

MS-13 has its own “law enforcement” mechanisms by which underperforming or failing members face a “court” held by their peers. This court determines the appropriate punishment based on the offense of the member. According to one report, the punishment could be one of three options: a 13-second beating, a 26-second beating, or a 36-second beating. In cases where gang members cooperate with law enforcement, punishment by death is the clear option.[162]

F. VULNERABILITIES AND CONCLUSION

MS-13 is a good example of a Type-I dark network in the sense that it followed the basic principles of dark network design for its design state. It is well configured with the following exceptions. Specifically, MS-13 does not adequately address the principles of security, capacity, agility and resilience.

[160] Sam Logan, Ben Bain and Kate Kairies, “Deportation Feeds a Cycle of Violence in Central America,” *World Press*, March 31, 2006, http://www.worldpress.org/Americas/2304.cfm (accessed on July 11, 2010).

[161] Sullivan and Logan, “MS-13 Leadership

[162] See Vaughan and Feere (2008) and Harness (2006) for more examples of the MS-13 “court” system.

First, MS-13 violates the principle of security. In a network where membership is nearly unrestricted and the requirement for secure coordination of work is moderate, there are multiple opportunities for interdiction. Since MS-13 is less concerned with security than rapid growth and conducting action, admission into the gang is not restricted. Once recruits are willing to be "jumped-in" and prove their loyalty, they are in. MS-13 includes multiple nationalities and cultural backgrounds.   If recruits can further the cause of MS-13, appealing to its reputation as the World's Most Dangerous Gang, they can join. This makes the gang vulnerable to penetration by not only law enforcement agencies, but also members of other dark networks, such as al-Qai'da or Hezbollah, that may seek to exploit MS-13's vast smuggling network to illegally enter the United States. If MS-13 is linked to terrorist organizations, then environmental hostility could increase exponentially.

MS-13 also violates the principle of security with their lack of concern over detection. This lack of concern stems from the fact that law enforcement efforts to combat them is not coordinated. This lack of coordination exists both within the United States and with the partner nations with MS-13 activity. The gang would be less resilient if faced with a more coordinated effort versus the limited regional approach that currently exists.

Second, MS-13 violates the principle of capacity. Many members are drawn to the gang merely due to lack of alternatives. MS-13 offers a code, structure, and a family to disaffected poverty stricken, directionless youth. Programs in Mecklenburg, VA have already shown progress in reducing gang membership in one of the largest MS-13 clique locations. An increase in such alternatives along with a coordinated effort across the United States and internationally (this includes reforms in the current deportation process which has proven to be more of a aid to the gang than a hindrance) could prove detrimental to further growth and success of MS-13.

Third, reports have begun surfacing that MS-13 may be attempting to create a national command structure across the United States. For a Type-I dark network configuration, this is a trade-off where exerting more centralized control results in the violation of the principle of agility. Becoming more centralized makes them less agile and more vulnerable to key target interdiction.

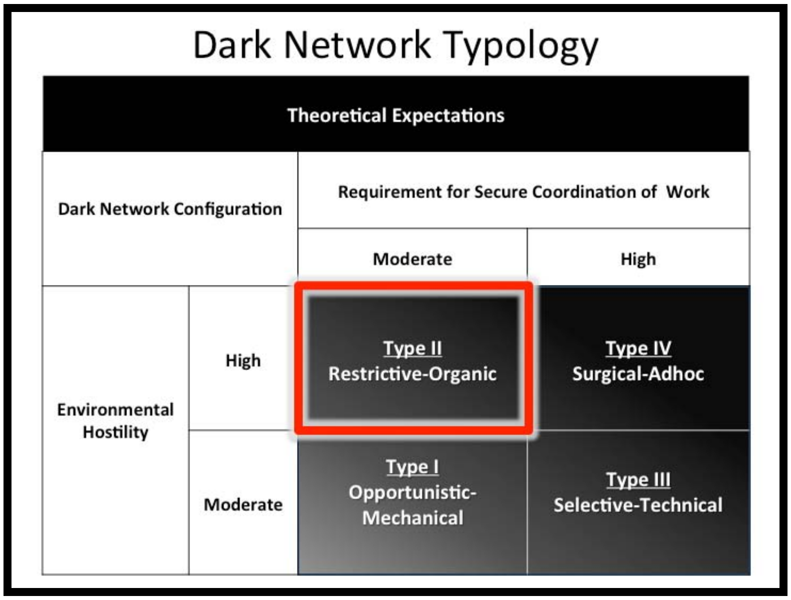
Finally, an inherent vulnerability lies in mechanical configuration of a dark network like MS-13. The loose-autonomous cells and decentralized action, while very adaptable and flexible for the network, also allow for simple misinformation to bring the network down. Since the geographically defined MS-13 cliques to not all communicate with each other, it is possible they may not even know who the big players in the larger cliques (Los Angeles and N. Virginia) are. Direction can be given to these smaller cliques to change action, change targets, or remove certain gangs from the "enemies" list in an effort to begin to reduce the levels of violence. A network with this configuration is highly susceptible to penetration and information operations.[163]

This chapter illustrated a Type-I Dark Network configuration: Opportunistic-Mechanical through the depiction of Mara Salvatrucha 13. The opportunistic action and mechanical configuration allows this type of dark network to choose the most profitable crime for its given location while allowing for a directional configuration that allows each clique to operate as it sees fit in a given environment. The configuration allows for great freedom of action, but it also leaves the network highly susceptible to illumination and interdiction. It is the will and capacity of the regional law enforcement agencies as well as the lack of a coordinated effort that limit the successful interdiction of this type of dark network.

[163] For more information on offensive information operations, see Edgar A. Jimenez, James S. McCullar and Kevin M. Trujillo, *Pseudo Operations and Deception in Irregular Conflict*, (Monterey: Naval Postgraduate School, 2010).

V. TYPE-II DARK NETWORK: RESTRICTIVE-ORGANIC

A. INTRODUCTION



Dark Network Typology

Theoretical Expectations			
Dark Network Configuration		Requirement for Secure Coordination of Work	
		Moderate	High
Environmental Hostility	High	Type II Restrictive-Organic	Type IV Surgical-Adhoc
	Moderate	Type I Opportunistic-Mechanical	Type III Selective-Technical

Figure 20. Restrictive Organic Dark Network

The purpose of this chapter is to illustrate an example of a dark network whose design state is defined by high environmental hostility and a moderate requirement for secure coordination of work that yields what we call Type-II Restrictive-Organic configuration. Based on our theory of dark network design, the example shows how a Restrictive-Organic dark network is configured to achieve its purpose and how it is vulnerable to illumination and interdiction.

Type-II dark networks can be the underground elements of a revolutionary movement that maintain a clandestine and covert lifestyle, emerge to conduct decisive action, and then return to the underground to avoid destruction. These dark networks may remain geographically dispersed and apply layered security measures to buffer hostility. There are many modern examples of networks that have a Restrictive-Organic configuration: Indonesia's Jemmah Islamiyah (JI), the Haqqani network in Afghanistan and Pakistan, and the South Florida-based anti-Castro movement Alpha 66.

For our illustration of a Type-II dark network configuration, we use the ethno-nationalist insurgent network of the Provisional Irish Republican Army (PIRA). We selected it over the others because of its transnational in nature; it most closely illustrates the typological design state of a Type-II dark network; and its prominence that provides a rich collection of open-source information on the dark network.

B. OVERVIEW OF THE PROVISIONAL IRISH REPUBLICAN ARMY

The Provisional Irish Republican Army (PIRA), or *Óglaigh na hÉirean* in Irish, is a ethno-nationalist insurgent network based around Irish Irredentist goals. The stated goal of the PIRA, nicknamed the "Provos," was to end British rule of the six counties in Northern Ireland and unite the north with the Republic of Ireland. Though its goals were localized, its reach was transnational, utilizing the North American Irish Diaspora and the international terrorist community to develop a robust financial and material support network. The PIRA formed in Northern Ireland in 1969 after a split from the main body of the Irish Republican Army over ideological issues and direction of the strategy of liberation.

Throughout its history, the PIRA waged a protracted campaign of popular warfare against British forces in the face of British national and regional security services, as well as opposition protestant terrorist organizations, such as the Ulster Defense Force (UDF). During the course of its armed campaign, estimates calculate that the PIRA killed approximately 1,800 people, including approximately 1,100 members of the British security forces.[164]

[164] "Provisional Irish Republican Army" *Jane's World Insurgency and Terrorism*, Jane's Terrorism and Insurgency Center (2009), http://www8.janes.com.libproxy.nps.edu/JDIC/JTIC/documentView.do?docId=/content1/janesdata/binder/jwit/jwita107.htm@current&pageSelected=&keyword=&backPath=http://jtic.janes.com/JDIC/JTIC&Prod_Name=JWIT&activeNav=http://www8.janes.com/JDIC/JTIC (accessed on September 28, 2010)

C. TYPE II DESIGN STATE

1. High Hostility of the Environment

The Type-II dark network operates in an environment with a high level of hostility. A high level of environmental hostility exists when opposition elements possess the will and/or capacity to counter the dark network. Opposition elements can commit varying degrees of resources to either suppress or destroy the dark network. In the case of the PIRA, British and Loyalist forces efforts to eliminate the Provos dominated the environment. Although the active members of the PIRA numbered about 400, they faced about 32,000 police and military force arrayed against them.[165] The forces of the United Kingdom had international legitimacy on their side and used the legal system as a tool to limit the spread of the Provos influence. Initially, the PIRA had a strong sense of legitimacy in the Catholic nationalist population and other Irish-Catholic diaspora throughout the world, but British security forces developed overt and covert mechanisms over time to undermine the PIRA's embeddedness in the population and maintain pressure on their networks.

The British military forces and Royal Ulster Constabulary (RUC) conducted simple police work and overt tactical operations—such as roving check points, raids, and surveillance—in order to keep violence to a manageable level.[166] The persistent presence of security forces throughout the operational area of the North and their coordination with the Guardia, the Irish Republic Police, kept the PIRA on the defensive. Further, the use of clandestine methods such as agent infiltrations and electronic eavesdropping were effective for infiltrating some of the PIRA's operations.

The Provos also had rivals in the covert and clandestine world. Loyalists formed citizens' defense groups to counter the growing influence of the PIRA and

[165] J. Bowyer Bell, *The Secret Army*: *The IRA,* Rev 3rd Ed. (New Brunswick: Transaction Publishers, 1997), 435.

[166] J. Bowyer Bell, "Dragonworld (II) Deception, Tradecraft and the Provisional IRA," *International Journal of Intelligence and Counterintelligence*, 8, No. 1 (1995), 40.

associated nationalist extremist groups. Groups like the Ulster Defense Association (UDA) and Ulster Volunteer Force (UVF) were responsible for more civilian casualties, usually those involved with supporting Catholic causes, than any other groups in the North.[167] These loyalist groups were also involved in organized crime as a method of fundraising, which increased the points of competition, contention and rivalry with the PIRA.

2. Moderate Requirement for Secure Coordination of Work

Type-II networks have a moderate requirement for the secure coordination of work because they maintain sanctuaries within the diaspora that are sympathetic to their activities and provide a space for operational planning and resourcing. These sanctuaries provide temporary “safe areas” to escape environments with a high level of hostility. This popular support base gives the network its resiliency. Opposition elements find it difficult, but not impossible, to penetrate theses sanctuaries in an effort to illuminate and interdict the dark network. Since the risk of compromise still exists inside and outside of the sanctuaries, Type-II dark networks will employ moderate levels of clandestine and covert behavior and conduct decisive action using compartmented cells. Operating from sanctuaries in small elements allows the dark networks to the maximize secure coordination of work with a minimum expenditure of resources.

The state’s concern about the rule of law and the perceived legitimacy of actions conducted state-sponsored oppositional elements can reduce the dark network’s requirement for secure coordination of work. Since the level of repression by opposition elements was limited by the British legal system, the PIRA had a moderate requirement for secure coordination of work because it did not expect the application of Draconian control measures. British society, with its interest in civil liberties, prevented the security forces from the use of effective repression and the use of widespread internment of known PIRA suspects. The singular attempt at developing a limited gulag-style internment system in 1971

[167] Andrew Silke, “In Defense of the Realm: Loyalist Terrorism in Ireland Part 1: Extortion and Blackmail*,” Studies in Conflict and Terrorism*, 21 (1998), 335.

was a failure and political disaster for the United Kingdom.[168] Although opposition elements may be constrained by rule of law to maintain legitimacy, they may have the will and capacity to commit extensive intelligence, military, and law enforcement assets to illuminate and interdict the dark network. Therefore, Type-II dark networks must develop appropriate mechanisms for secure coordination of work.

The British Security Services were very adept in using the latest electronic eavesdropping technology. Thus, telephonic communication, no matter how cryptic, was very perilous. Personal clandestine communication was also hazardous. Therefore, the PIRA used basic non-technical impersonal communication techniques, such as emissaries or messengers, to pass information in short notes to conduct operations.[169] These basic procedures provided a moderate level of secure coordination of work with a minimum expenditure of resources.

D. TYPE-II DARK NETWORK: RESTRICTIVE-ORGANIC

We characterize Type-II dark networks as restrictive and organic for the following reasons:

1. Restrictive Action

Since the environment is has a high level of hostility, the network must restrict actions to those that are most effective and necessary for long-term survival. Hostility influences action; limiting how, when, and where the network can act; and how successfully it can mobilize its support base. To protect itself and build operational capacity, the network establishes sanctuaries from which to organize, plan, and recover from operations. As mentioned earlier, these sanctuaries are nested within sympathetic populations that provide both active and passive support. The strategic core uses the sanctuary to set the direction

[168] Bell, “Dragonworld (II) Deception, Tradecraft and the Provisional IRA,” 42.

[169] Ed Moloney, *A Secret History of IRA*, 2nd ed., (London: Penguin Books, 2007), 161.

and frame the purpose of the network in a manner that resonates with the members of the network and the population. Meanwhile, the functional periphery directs and executes decisive action and support activities through its compartmented cellular structure and secure coordination infrastructure. Restricting action permits the dark network to conserve resources and develop the capacity to conduct decisive action to achieve its purpose in a hostile environment.

2. Organic Configuration

In the organization design sense, an organic configuration is characterized by: [170]

- Flatness: communications and interactions are horizontal;
- Low specialization: knowledge resides wherever it is most useful, and;
- Decentralization: great deal of formal and informal participation in decision-making.

From a dark network paradigm, the organic network that operates in an environment with a high level of hostility seeks to minimize the number of connections between core and peripheral components to maximize security. Thus, organic networks may set direction by disseminating a clear intent to be executed the dark network's decentralize peripheral elements. Network fail-safe mechanisms enable the secure coordination of work and allow the network to rapidly adapt to a dynamic, hostile environment. Furthermore, the organic configuration allows the network to coordinate work in a secure manner over a wide geographical area, without the need for constant communications between the strategic core and peripheral operational and supportive elements.

[170] Organic organizations are comparatively more complex and harder to form, but are highly adaptable, flexible, and more suitable where external environment is rapidly changing and is unpredictable. Also called open organizations, they are contrasted with mechanistic organizations. See Web Finance Incorporated, Organic Organization Definition, November 26, 2010, http://www.businessdictionary.com/definition/organic-organization.html (accessed November 26, 2010).

E. FUNDAMENTAL COMPONENTS

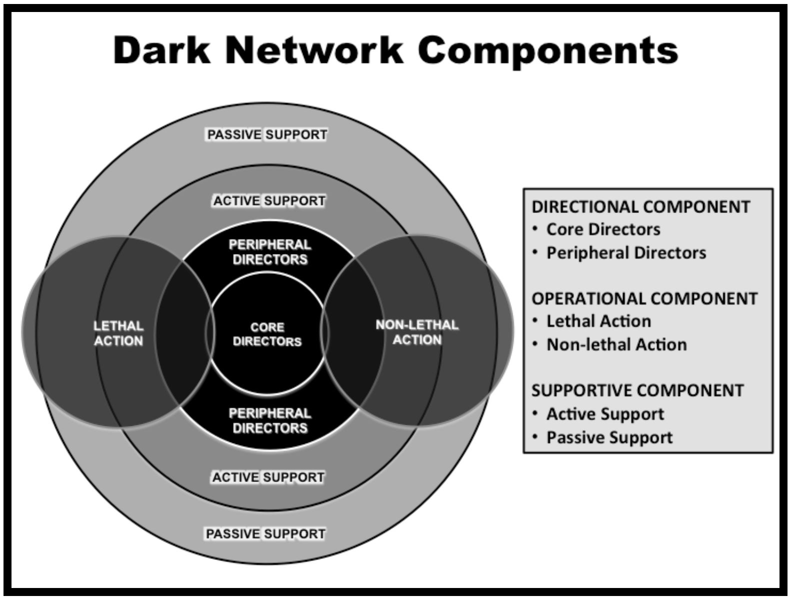


Figure 21. Illustration of Dark Network Components

1. Directional Component

The configuration of the PIRA's directional component evolved because of network/organizational learning that drove them to relinquish a hierarchal form of organization for an agile networked structure. The directional component of the PIRA originally mirrored conventional command hierarchy that had served the IRA through its push for Irish republican independence and the limited civil war. The PIRA *morphed* its configuration to a hybrid hierarchy/cellular network model after the 1974 cease-fire, when they realized that they were vulnerable to infiltration.

Since British the security apparatus was highly practiced at penetration operations, the PIRA adopted a compartmentalized cellular network configuration to create a system of limited communications, which would limit the exposure of the PIRA directional component. In this system, the Officer Commanding (OC) of the operational unit, known as the Active Service Unit (ASU), would serve as the secure link to the core directors of the directional component. As Horrigan and Taylor observed:[171]

> Each Volunteer in theory only knows the identity of the OC. Each OC in theory knows only one higher authority, which is the Brigade Adjutant, who receives orders from a member of the GHQ [General Headquarters]/Army Council/Northern-Southern Command grouping.

The overt elements of the PIRA/IRA, along with GHQ, represented the core directors. The OCs represented PIRA's peripheral directors. For security purposes, the strategic key actors were detached from the peripheral key actors; locating in areas of known sanctuary that offered it the ability to conduct work with a limited threat of interdiction. This limited communication forced the PIRA GHQ into a role of oversight with out control and allowed the ASUs greater autonomy (Figure 24).

The core directors successfully tapped generations of resentment, humiliation and societal frustration by focusing on the strategic objectives of redressing a historic injustice. This struggle for justice was the motivation that kept the "Provos" focused for 30 years of violent struggle.

The PIRA articulated its overall strategic objectives to it members in *The Green Book*; a field training manual and policy manifesto that was used to indoctrinate new PIRA Volunteers: [172]

1. A war of attrition against enemy personnel which is aimed at causing as many casualties and deaths as possible so as to create a demand from their people at home for their withdrawal.
2. A bombing campaign aimed at making the enemy's financial interest in our country unprofitable while at the same time curbing long term financial investment in our country.

[171] John Horgan, and Max Taylor, "The Provisional Irish Republican Army: Command and Functional Structure", *Terrorism and Political Violence*, 9: 3 (1997), http://dx.doi.org/10.1080/09546559708427413 (accessed on October 20, 2010), 20.

[172] Jackson et al., *Aptitude for Destruction*, 95.

3. To make the Six Counties as at present and for the past several years ungovernable except by colonial military rule.
4. To sustain the war and gain support for its ends by National and International propaganda and publicity campaigns.
5. By defending the war of liberation by punishing criminals, collaborators and informers.

The core directors set strategic policy, managed the PIRA's ideology, dealt with macro level sustainment issues, and coordinated for international support. PIRA's core directors also controlled the transnational element of the strategy. This transnational element focused on developing a bombing campaign in the Great Brittan and targeting British interests in Europe.[173]

Along with the development of the cellular structure came the development of a more stable and static underground leadership which replaced the outmoded hierarchical Brigade system of the PIRA's predecessors. This development of the underground Army Council intended to provide strategic direction setting and a General Headquarters (GHQ) to conduct the macro scale coordination of operations, support, intelligence, to coordinate transnational activities. This structure gave the PIRA a static cadre of key actors, who would focus strictly on supporting a protracted popular war of attrition.[174] Under the GHQ, the PIRA developed a Northern Command, a peripheral director, that would coordinate with the ASUs to ensure they were working towards the same intent. The node coordinated action and enforced PIRA directives. A similar node was established in the South to coordinate active and passive support activities. GHQ and Northern Command tried to exercise operational control by managing the distribution of weapons and finances, but this mechanism became vulnerable to infiltration (Figure 24).[175]

[173] Jackson et al., *Aptitude for Destruction,* 116.

[174] Moloney, *A Secret History of the IRA*, 158.

[175] Jackson et al., *Aptitude for Destruction* 134.

The peripheral directors of the PIRA's directional component consisted of the various OCs that were dispersed throughout the network. These OCs were responsible for taking ideology and intent and turning them in to quantifiable results through the actions operational element (Figure 22).

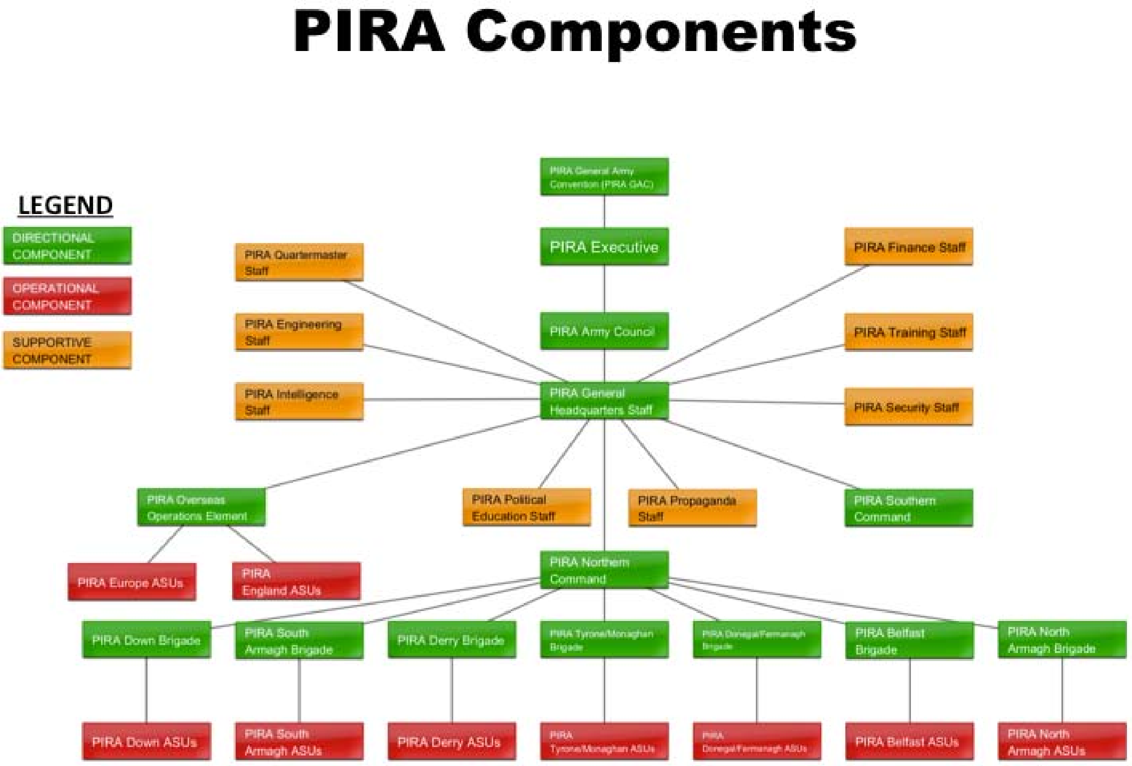


Figure 22. Illustration of PIRA Components Visualized in Palantir.[176]

In an attempt to keep ASU operations focused on British and Loyalist security forces and mitigate sectarian violence, the directional component shaped its strategic message to indoctrinate its members and the world audience that the PIRA was conducting a legitimate war of national liberation.[177] PIRA's

[176] Graphic derived by authors' interpretation of Horgan and Taylor, "The Provisional Irish Republican Army: Command and Functional Structure."

[177] Robert W. White, 'Don't confuse me with the facts: More on the Irish republican army and sectarianism', *Terrorism and Political Violence*, 10 no. 4, (1998)164–189, http://dx.doi.org/10.1080/09546559808427487 (accessed October 1, 2010).

political wing, *Sinn Fein* (Ourselves Alone), set direction for the network and ensured that the PIRA ASUs considered the political objectives of mobilizing the Irish-Catholic ethno-centralism to win at the ballot box, as well as acts of calculated violence aimed at portraying the British as ineffective and incapable of providing security. In order to maximize the political benefit of the duel political and armed struggle strategy promulgated through the "Armalite and Ballot box" paradigm, the strategic core exerted increasing control over the ASUs.[178] The strategy was to nest ASU activities with the greater goals of the political wing. By 1986, Northern Command retained approval authority for any ASU seeking to execute an operation.[179] This development sapped much of the creativity and unpredictability away from the ASUs by the early 1990s.

2. Operational Component

The PIRA's Active Service Units (ASUs) formed the core of its operational component and were responsible for conducting decisive action using both lethal and non-lethal means. As a mentioned earlier, the PIRA adopted a cellular networked structure to conduct decisive action in early 1970s. These cells were limited to four people; had a specialty, such as bombing, sniping or robbery; and were commissioned to operate regionally in order to widen their operational pattern. [180] These cells became the decisive action elements of the PIRA, which were all-channel cells of between eight and twelve members. The PIRA's operational concept initially allowed for great flexibility and bottom driven activities. ASUs had the latitude to generate their own operational plans and support mechanisms at the local level, which will be discussed later.

The PIRA's operational component ensured operations were nested with the intent of the directional component's strategic message. This provided unity

[178] John A. Hannigan "The Armalite and the Ballot Box: Dilemmas of Strategy and Ideology in the Provisional IRA," *Social Problems*, 33, No. 1 (Oct., 1985), 31–40, http://www.jstor.org/stable/800629 (accessed May 10, 2010).

[179] Moloney, *A Secret History of IRA*, 317.

[180] Tim Pat Coogan, *The IRA*, (London: Harper Collins, 2000), 466.

of effort across the decentralized ASUs. Thus, the PIRA's organic configuration and compartmentalized cellular structure was effective in thwarting British attempts at interdicting the ASUs. The Irish Police Service (Gardai) were frustrated by the this cellular compartmentalization: "We know the key personnel and activists and sympathizers who have come to our attention, but the cell structure is so tight that their own members wouldn't know the make-up of other cells."[181] When ASUs did work together, they coordinated operations through a liaison. To maintain security, Volunteers used only first names or aliases. As an additional security measure to confuse opposition elements, the PIRA would put younger, unknown Volunteers in positions of operational responsibility, while the higher profile members would become front men for more legitimate segments of the movement, such as *Sinn Fein*.

3. Supportive Component

The PIRA's supportive component conducted active and passive support activities from the local to the international level. The ASUs often develop their own direct support cells within the local area to get what they need on a day-to-day basis. The level of support varied widely depending on the tactical situation. Many ASUs depended on popular support within the sanctuaries and their own creativity to build infrastructure required to generate an ASU's operational capacity. The Provos' vast support infrastructure included warehouses, safe houses, and caches throughout the 32 counties of the Republic of Ireland. The PIRA also relied on allies in the United States, Basque separatists in Spain, and the regime of Momar Quadaffi to supply weapons and raw materials to equip their volunteers. [182]

The supportive component played a critical role in establishing and maintaining sanctuaries that provided a base of ideological and material support in both rural and urban settings. The amount of popular support in a given area

[181] Horgan, and Taylor, "The Provisional Irish Republican Army," 22.

[182] James Adams, *The Financing of Terror*, (New York: Simon and Shuster, 1986), 6.

often determined the operational capability of the local Provo units. Many of the nationalist neighborhoods in the urban environment were “no-go” zones offered an environment where the opposition forces could not operate freely, thus mitigating the hostility in the environment and giving the opportunity to maintain a Provos a persistent presence. These sanctuaries offered both active support and a general “halo” of toleration; a buffer of tactic support from sympathetic populations.[183] Beyond these pockets of sanctuaries in urban centers such as Belfast, the rural environment offered pockets of strong support. The border between the Republic of Ireland and Northern Ireland offered an ease of passage which allowed volunteers and material to transit the two regions. This gerrymandering of sympathetic populations allowed for the PIRA to move through areas of sanctuary throughout the countryside.

The use of sanctuaries was vital to the active support of the PIRA. The GHQ was located in Dublin, the PIRA quartermaster lived and worked in the Republic of Ireland, and many of the ASUs concealed themselves in neighborhoods or regions in the North that the PIRA controlled.[184] This geographic sanctuary allowed for operational and support elements to conduct their work and learn best practices over time, with a reduced incidence of interception by hostile forces. The PIRA focused most of their cache activities, improvised weapons manufacturing, and training camps in the Republic of Ireland under the auspices of the Southern Command.[185] This sanctuary was possible due to the PIRA’s cultural embeddedness in the Irish-Catholic population. Many of the disenfranchised Catholic minority in the North—a sizeable minority in the Republic of Ireland—and many of Irish descent in the international Diaspora shared the network’s goal of a unified Ireland free of

[183] Bell, “Dragonworld (II) Deception, Tradecraft and the Provisional IRA,” 35.

[184] Jackson et al., *Aptitude for Destruction,* 95.

[185] Moloney, *A Secret History of the IRA,* 158.

British influence. Because of this ideological connection with the Irish cultural mindset, the PIRA was able to maintain a steady of flow of volunteers, weapons and money.[186]

The supportive component also established an elaborate communications and early-warning system. Many of the impersonal communication measures were very simple non-technical means of conveying information. One example of these impersonal means of communications occurred when sympathizers who lived in a tall apartment building would spot approaching patrols with binoculars and they would hang a towel on their balcony or open a window to indicate that the security forces were in the area.[187] The PIRA also used dead-drops, a type of cut-out, to indirectly the transfer written messages, as a method to limit exposure to British or Loyalist intelligence collection measures during operations.[188]

Although the PIRA generally used lower technology solutions for transmitting information, there were instances that illustrated the PIRA's desire to utilize higher technology to make their support of operations more efficient. In 1979, the RUC "discovered a hidden command post filled with radios, unscrambling equipment, sophisticated monitors, military style transmitters, position fixing devices and telephone taps routed through British Telecom network."[189] The PIRA used this equipment to eavesdrop on the British security services in order to stay a step ahead of them. The use of advanced electronic devices, those rare were effective for PIRA operations and intelligence.

For the PIRA, security was a paramount issue for the support elements and led to the development counterintelligence elements to ferret out informers and spies. British and Loyalist security services were constantly infiltrating the

[186] Bell, "Dragonworld (II) Deception, Tradecraft and the Provisional IRA," 35.

[187] Jackson et al., *Aptitude for Destruction* 128.

[188] Bell, "Dragonworld (II) Deception, Tradecraft and the Provisional IRA," 43.

[189] Bell, *The Secret Army: The IRA*, 473.

network in an attempt to illuminate and interdict the PIRA. To counter this threat, the PIRA GHQ developed a security cell, which, was responsible for aggressive, independent, counterintelligence operation. This security cell was chartered to rooted out informants and vet new recruits into the network.[190] In addition to hunting informants and vetting new recruits, the cell investigated security breaches and reviewed every botched mission to ascertain the likelihood that a security breach was the cause of the failure.[191] This cell, known for its brutal interrogations in search of informants, had a ruthless clique known as the "nutting squad" that were known for shooting people in the head.[192]

Ironically, the Provos' most vulnerable element was the security cell. The cell had the most extensive knowledge of the PIRA's cellular organization, down to the recruit level, and the British Security Services made it a priority to infiltrate this element. The British had at least three major sources within the security cell, two of whom were formerly in charge of the cell.[193] One of the most damaging of these informants was Freddy "Scap" Scappaticci, the director of the security cell throughout the 1980s.[194] From his vantage point he had knowledge of Volunteer identities, IRA operations and support networks.[195]

The PIRA's ability to finance operations was critical element for overall sustainability and used a loose collection of individuals that constituted their "finance department."[196] This finance department worked to find every angle, both licit and illicit to raise money for the movement. The PIRA often used a cover for overt fundraising that went to funding decisive operations. The PIRA

[190] Moloney, *A Secret History of IRA*, 335.

[191] Moloney, *A Secret History of IRA*, 335.

[192] Jackson et al., *Aptitude for Destruction,* 11.

[193] Moloney, *A Secret History of IRA*, 575.

[194] Ibid., 575–577.

[195] According to Moloney, Scapaticci had volunteered his services to the British security services after he had received a severe beating at the hands of some PIRA colleagues. These volunteers were the most effective and reliable sources within the PIRA.

[196] John Horrigan and Max Taylor, "Playing the Green Card: Financing the Provisional IRA, Part II," *Terrorism and Political Violence,* 15, No. 2 (Summer 2003), 7.

used front companies, like taxi companies, pubs, and drinking clubs in the North and in Republic. Taxi companies and security firms were not only lucrative forms of financing, but also employed many volunteers, provided social services and provided cover for PIRA illicit activities.[197] Many of these businesses would have PIRA accountants who could fiddle with the tax returns in order to funnel unaccounted for money to the PIRA.

The PIRA's support elements also consisted of a vigorous transnational support element. The PIRA was dependent on its international relationships to supply the organization with weapons. The PIRA developed a strong relationship with the government of Libya, who supplied advanced weapons, explosives and hosted training events for PIRA volunteers.[198] The PIRA also interfaced extensively with the Basque Fatherland and Liberty Party (ETA), who not only supplied the PIRA with weapons, but also pooled ideas, technology and training.[199] Irish Republican sympathizers in the United States generated the most robust international support for the PIRA, collectively supplying the network with millions of dollars and the earliest supplies of assault rifles in the form of the Armalite AR-15.[200] The largest contingent of American support came from an overt New York based group of sympathizers called Irish Northern Aid, or Noraid. Under the guise of a charity for the families of imprisoned PIRA Volunteers, Noraid supplied nearly half of the PIRAs operating budget in the early years of the network.[201]

F. CONCLUSION AND VULNERABILITIES

The PIRA is a good example of a Type-II dark network in the sense that it was able to achieve its purpose despite the commitment British national assets to counter it. The PIRA managed to configure itself and follow the principles of dark

[197] James Adams, *The Financing of Terror*, (New York: Simon and Shuster, 1986), 174.

[198] Jackson et al., *Aptitude for Destruction,* 120.

[199] Ibid.

[200] Adams, *The Financing of Terror*, 142–143.

[201] Ibid., 136.

network design. Its structure evolved to protect the operational wing of the movement while retaining a modicum of control and generating a robust support network. Despite PIRA's surviving in a hostile environment for over thirty years, the network did have vulnerabilities that were partially responsible for limiting its overall capacity. Specifically, the PIRA violated or did not adequately address the principles of security and agility.

First, in terms of the principle of security, PIRA centralized its security enforcement and counterintelligence apparatus in an effort to gain greater control, and to protect the network. This apparatus had knowledge on the composition of the cellular network. The broad knowledge base of this entity made it a tempting target for penetration by British and Loyalist forces. As a result, PIRA's security cell became a single point of multiple devastating security breaches.

Increased efforts to control and coordinate strategy and operations could also created security lapses. Since the PIRA conducted much of its coordination through the passing of indirect messages, a poorly worded note led to misunderstanding and failure. Furthermore, compromised messengers or dead drops, led to the interception of operational plans and the planting of deception traps for the ASUs.

Additionally, in developing stronger control measures, Northern command would occasionally force ASUs into sharing information and breaking their strict compartmentalization. There were circumstances wherein Northern Command forced ASUs to coordinate and work together, even when it was a bad idea. In one case, the ASU in South Armagh had developed a remote controlled detonator for their roadside bombs, which they did not want to share, as they feared the British would develop and effective countermeasure. Northern

Command forced the South Armagh ASU to share its technology with the rest of the network, and the British were able to discover it and developed an effective countermeasure.[202]

Second, the PIRA violated the principle of agility. The PIRA limited its network agility by attempting to maintain too much control over its disparate network cells. As the PIRA looked at the increasing success of their political agenda, they needed to ensure that the ASUs were conducting operations that were in-line with the long-term political objectives. Over time this control lead to the lessening of initiative at the OC level and a loss of effectiveness.

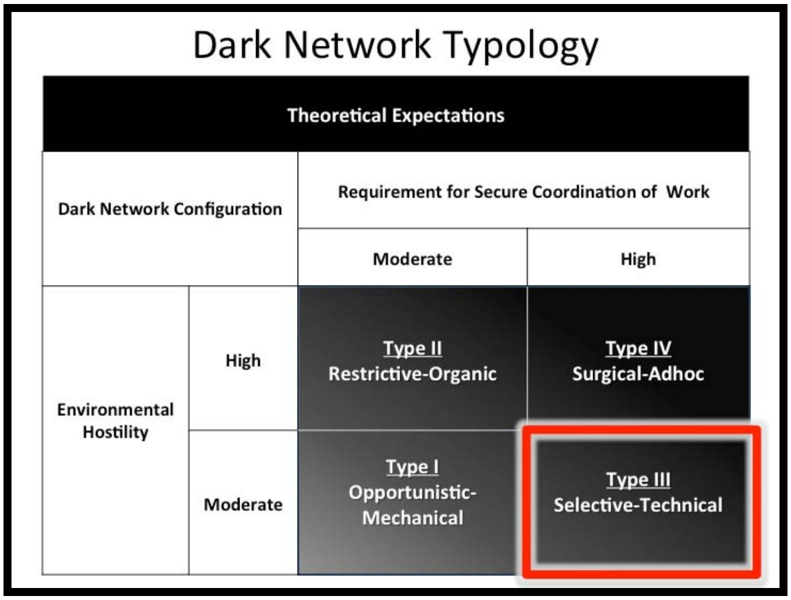
In conclusion, Restrictive-Organic networks can be very effective forms of organizing armed resistance, but they are still vulnerable. This network has an ability to plan and support operations, raise funds, and is deftly adaptive at mitigating the countermeasures of the oppositionist forces. Those restrictive organic networks that have been the most successful were those who were able to develop areas of sanctuary that allowed permitted a safe environment for the directional component plan and coordinate operations and for the network to generate a base of ideological and material support.

As an example the Restrictive-Organic dark network, the PIRA was effective in maintaining its efforts over the span of three decades. But as the network evolved, experienced early success, and grew, the strategic core attempted to exert an increasing amount of control over the distributed cellular ASUs. This focus on control sapped the network of effective security measures and network agility.

[202] Moloney, *A Secret History of the IRA*, 161.

VI. TYPE-III DARK NETWORK: SELECTIVE-TECHNICAL

A. INTRODUCTION



Dark Network Typology

Theoretical Expectations

Dark Network Configuration		Requirement for Secure Coordination of Work	
		Moderate	High
Environmental Hostility	High	Type II Restrictive-Organic	Type IV Surgical-Adhoc
	Moderate	Type I Opportunistic-Mechanical	Type III Selective-Technical

Figure 23. Type-III Dark Network Quadrant

The purpose of this chapter is to illustrate an example of a dark network whose design state is defined by a high requirement for secure coordination of work and moderate environmental hostility that yields what we call a Type-III: Selective-Technical dark configuration.

Type-III dark networks can include the auxiliary component of an insurgent network, material supply chains, personnel recovery mechanisms, or other support networks that provide material and financial support to revolutionary movement. Historical examples of this type of network include the French Resistance Allied pilot evacuation network in occupied Europe during World War II, al-Qa’ida’s training and support operations conducted in the Sudan in the mid 1990s, and the global support network for Islamists conducting the global Salafi jihad.

For our illustration of a Type-III dark network configuration, we use Hezbollah's transnational support network, with a special emphasis on its operations in the Americas. Hezbollah is multifaceted radical Shiite movement that conducts both licit and illicit activities throughout the world to achieve its purpose. We chose Hezbollah because it is a transnational network with vast amounts of information available for research. It also most closely illustrates the typological design state of a Type-III dark network.

B. OVERVIEW OF HEZBOLLAH

Hezbollah[203], or “Party of God,” originally formed in 1982 in the Bekaa valley of Lebanon. It was created as reaction to the Israeli invasion of Lebanon and was initially composed of small radical Shia groups inspired by the 1979 Islamic Revolution in Iran. Most of its early leaders had connections to the Shia seminaries in Najaf, Iraq, where they were inspired by the radical teachings of Mohammed Baqr as-Sadr and Ayatollah Ruhollah Khomeini.[204] Born in conflict, Hezbollah’s stated goals remain rooted in revolutionary thought. The pillars of Hezbollah’s philosophy are the empowerment of Shiite nationalism in Lebanon and active resistance to the regional influence of state of Israel and its allies.[205]

Hezbollah is one of the most powerful and diverse terrorist networks in the world. It has the capacity to conduct a wide range of military activities from asymmetric, attacks such as suicide bombings and kidnappings, to more conventional large unit tactics, as seen in its limited war with Israel in 2006. Although Hezbollah is primarily viewed as a terrorist group by most of the world, it has also spent decades building a social service capability. Hezbollah has won

[203] There are multiple spellings for the transliteration of this name الله حزب in to English ,to include Hizbollah, Hizballah, Hizbullah, Hezb’ Allah. For the purposes of this chapter, the group will be referred to as Hezbollah. Arabic translation from http://en.wikipedia.org/wiki/Hezbollah

[204] “Groups - Middle East – Active – Lebanon: Hizbullah” *Jane’s World Insurgency and Terrorism Website*, 29 April 2010, from http://www4.janes.com.libproxy.nps.edu (accessed on June 4, 2010)

[205] National Counterterrorism Center, “Hizballah,” *Counterterrorism Calendar 2010,* “Groups,” http://www.nctc.gov/site/groups/hizballah.html (accessed on November 8, 2010).

a loyal support base through the provision of social services including health, education, and infrastructure in impoverished Shia areas during the decade long Lebanese civil war.[206]

Although its operations focus on actions in the Middle East, Hezbollah has branched out its networks internationally to develop an effective global support presence. One of the most important regions for Hezbollah's financial support has been through its development of operations throughout Latin America. Much of this expansion has been through the leveraging sympathetic elements in local Lebanese diasporas. These diasporas have been very successful in regional commerce, and weak governmental controls on banking and business gives Hezbollah the ability to move money and supplies through transnational smuggling routes. The Lebanese diasporas have become an important part of the fabric of the free trade zones in South America's Northern Cone. A large number of Lebanese moved to Latin America in 1948 after the Arab-Israeli War and again in the mid 1980's to escape the Lebanese Civil War.[207] Additionally, much of Hezbollah's Latin expansion has mirrored the spreading influence of the Iranian government in the region. Iran and Hezbollah use each other to expand their collective influence in the Western Hemisphere. For example, Hezbollah agents were linked to the 1992 bombing of the Israeli embassy and the 1994 bombing of the AMIA Jewish Center, both in Buenos Aries, Argentina[208]. The use of worldwide Lebanese diasporas helps Hezbollah conduct massive fund raising ventures and provides a vehicle for future operations.

[206] "Groups: Hizbollah," *Jane's World Insurgency and Terrorism Website*, http://jwit.janes.com/public/jwit/index.shtml (accessed on November 8, 2010).

[207] Arpoova Shah, "The Mullah, the Caudillo, and the Terrorist," *The American: The Journal of the American Enterprise Institute,* 1 April 2009, http://american.com (accessed on June 7, 2010).

[208] United States House of Representatives, Committee on International Relations, *Iran: A Quarter Century of State-Sponsored Terror,* (Washington DC: US Government Printing Office, 2005).

C. TYPE III DESIGN STATE

1. Moderate Hostility of the Environment

The Type-III operates in an environment that has a moderate level of hostility. Hostility is moderate because opposition elements lack the will and/or capacity to counter the dark network. The Type-III dark network operates in regions that are ill-governed and have a low capacity or will to enforce local laws or take the extensive measures necessary to interdict the dark networks. Against this backdrop the Type-III dark network is able to maximize its potential for accomplishment of purpose.

In the case of Hezbollah, the nature of the environment in Latin America presents a moderately hostile environment throughout the region. Latin America, like other regions dominated by developing economies, is ripe for exploitation by clandestine and covert organizations. This is due to endemic corruption, weak government institutions, ineffective or lack of intergovernmental cooperation, weak or non-existent legislation to deal with structural weaknesses, and a general reluctance to allocate adequate resources toward dealing with transnational terror and criminal groups. More commonly, the Selective-Technical operational component focuses on non-lethal operations to achieve their goal. Lethal or kinetic style operations tend to bring unwanted scrutiny from opposition groups and security forces. Selective action ensures that the network remains below the military horizon and does not generate increased hostility in the environment.[209] Lethal actions are usually only conducted as a defensive measure to protect supply lines, products, or to avoid destruction by opposition elements. The environment is moderately hostile to Hezbollah's illicit activities in Latin America because the local governments are not the specified targets of Hezbollah's lethal activities, despite pressure from the United States. Since

[209] Dark networks that rise above the military horizon often present themselves as legitimate targets for national security forces that have greater technological capabilities and combat power then local law enforcement entities. Staying below the military horizon allows a dark network to conduct their activities and hide in plane sight. For more information on the military horizon, see Harry Holbert Turney-High, *Primative War*, 2nd Ed. (Columbia: University of South Carolina Press, 1991), 21–38.

there is no immediate threat, Latin American nations simply lack the urgency to deal with the issues revolving around terrorism financing issues and activities.[210]

2. High Requirement for Secure Coordination of Work

Despite the moderate level of hostility in the environment, the Type-III dark network has a high requirement for the secure coordination of work. This high requirement is due to desire of the network to ensure the aforementioned environment remains at a moderate level of hostility. If their presence, or technology of work becomes known, the environment may become increasingly hostile. In the business sense, Type-III dark networks must protect their proprietary information if they are going to retain their competitive advantage over their rivals. Additionally, the high requirement for secure coordination of work is due to the sequential interdependence of the work that is conducted by the Type-III network. If one node of the network becomes compromised, repercussions will be felt throughout the rest of the network and can lead to catastrophic network failure. Therefore, redundant and loose coupled mechanisms, as well as clandestine and covert behavior, are techniques to enhance network security and resilience. A Type-III dark network generally conducts illicit activities to provide personnel, material, financial, and other support to develop capacity. By developing human, physical, and virtual infrastructure Type III networks enable capacity for future decisive operations. In the case of Hezbollah's Latin American cells, the focus on both licit and illicit activities as a method of generating funding invites the scrutiny of security services and rival illicit cartels, therefore forcing the network to maintain a high requirement for the secure coordination of work.

[210] Mark P. Sullivan, *Latin America: Terrorism Issues* (Washington DC: Congressional Research Service, 2009).

D. TYPE III DARK NETWORK: SELECTIVE-TECHNICAL

We characterize Type-III dark networks as selective and technical for the following reasons.

1. Selective Action

The Type-III network is selective in its action. This network is conducting selective actions in geographically disparate regions, filling a specific niche, to assist the efforts of the overall network's specifically defined end-state. These selective actions might be fundraising activities, but also might consist of recruiting, equipping, training or even operations to weaken the international stature of an opponent. In choosing specific areas such fundraising or recruiting, Hezbollah's operations in Latin America are selective in nature.

2. Technical Configuration

The Technical dark network often resembles a supply chain type of configuration that performs niche activities that typically require a high degree of technical skill or subject matter expertise. This supply chain formation is can be called technical interdependence, as the entire network is interdependent on all the cells being able to perform their technically specific tasks. The network operates in environments that have a moderate level of hostility and exploit the "white noise" afforded by local crime to conceal their true intent and enable the network to conduct lucrative operations with a modicum of opposition. Technical networks are generally configured to produce a specific result; such as moving licit and illicit commodities to market in order to generate funds, provide material support, and to build capacity of the network to achieve its purpose. The technical nature of these networks tends to cause the network to specialize in a niche and configure itself to optimize innovation and exploit the technical vulnerabilities of their intended targets.

E. FUNCTIONAL COMPONENTS

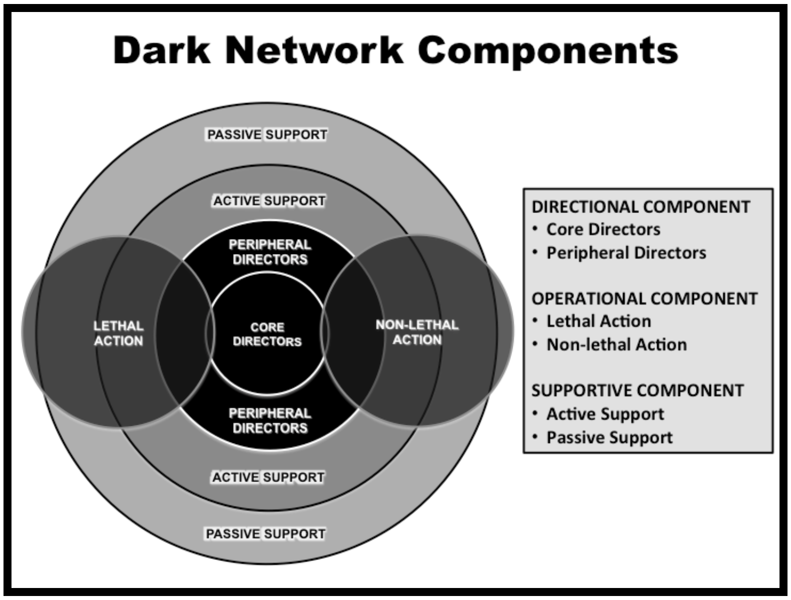


Figure 24. Illustration of Dark Network Components

1. Directional Component

Hezbollah's core directors in Lebanon set network's strategic direction and objectives. The core directors consist of a Secretary-General and a Deputy Secretary General who lead a seventeen member senior Shura, which oversees both the political and military wings of the militant group.[211] Hezbollah has the capacity to conduct operations across the world, such as those in Latin America, through the peripheral directors who are embedded in the diasporas. Additionally, Hezbollah has long been a proxy for the Clerical regime in Iran.[212] Hezbollah's core directors will often direct the network to on behalf of or in concert with Iranian interests.

[211] Brian A. Jackson, John Baker, Kim Cragin, Peter Chalk, John Parachini, and Horacio Trujillo, *Aptitude for Destruction: Case Studies of Organizational Learning in Five Terrorist Groups,* (Santa Monica, CA: Rand Corp, 2005), 38.

[212] Ely Karmon, *Iran and its Proxy Hezbollah: Strategic Penetration in Latin America Working Paper,* (Madrid: Elcano Royal Institute, August 2009), www.realinstitutoelcano.org (accessed on October 28, 2010), 15.

In Latin America, Hezbollah's cells maintain a member who focuses on *Dawa*, or missionary work. Utilizing pro-Hezbollah propaganda via local mosques, the cell will work to proselytize local citizens and build a stronger indigenous network thereby developing a stronger sense of embeddedness in the diaspora communities.[213] Like their compatriots in Lebanon, every unit has a religious or a "fighting cleric" element to enforce ideological adherence.[214] These "fighting clerics" who are all trained in the tactics of guerrilla warfare, maintain a connection to the Hezbollah religious authority and enforce the power of the *Shura* throughout of the network.[215]

2. Operational Component

Hezbollah's Latin American operational components likely follow the general template for Hezbollah's international action cells, which have three primary activities: 1) A *Dawa* and recruitment entity, based on Islamic clerics, religious centers and extremist propaganda; 2) A financing department whose capabilities based on the ability to raise money legally and illegally by using organized crime; 3) and an operational team, dealing with smuggling activists and means of warfare and the assembling of intelligence concerning potential targets.[216] Hezbollah's Latin American cells create long-term underground networks that develop operational plans and infrastructure, even as they are engaging in lucrative business ventures, both licit and illicit. This permanent planning capability gives the network's cells the operational agility to go from support to offense in at the most effective time, so they can maximize their results.[217]

[213] Cyrus Miryekta, "Hezbollah in the Tri-Border Area of South America" *Small Wars Journal*, September 10, 2010, http://smallwarsjournal.com/blog/journal/docs-temp/533-miryekta.pdf (accessed on October 25, 2010).

[214] Jackson et al., *Aptitude for Destruction*, 53.

[215] Ibid., 53.

[216] Eitan Azani, *Hezbollah: The Story of the Party of God,* (New York: Palgrave Macmillan, 2009), 204.

[217] Miryekta, "Hezbollah in the Tri-Border Area of South America."

Hezbollah places a high value on the virtue of self-sufficiency of the operational element. They launched a number of their best and brightest young operatives in to the Latin American region. These operatives, with no money and no outside assistance, deployed throughout Latin America to develop independent and compartmentalized networks with embeddedness in the local Lebanese and Arab diasporas.[218] By having regional redundancy, these networks increase their ability to penetrate local markets and gain both financial and operational access to important sectors of the region. By maintaining parallel circuit networks in the regional illicit trafficking market, Hezbollah maintains access to the same human trafficking routes that the drug smugglers use, allowing them to move operatives through the South and Central America at will.

Hezbollah and other The Type-III dark networks use several different methods to ensure secure coordination of work, of which compartmentalization can be a primary tool. This type of network sets its cellular network up in a circuit, through which materials travel or are transformed. If opposition forces manage to compromise one of these cells, the network cuts ties to that node, and the circuit adjusts to circumvent the loss. One method of attempting the secure coordination of work is by setting up parallel circuits as a redundancy measure. These parallel circuits are compartmentalized and are not aware of each other's existence. If one circuit is hampered, work-low can be shifted to another circuit. Type-III dark networks use elaborate deception to conceal their actual purpose from adversarial forces, for if their actions are discovered their infrastructure and activities can be easily interdicted, thereby eliminating the network as a viable structure. In the case of Hezbollah, the diasporas in Latin America engage in regional commerce through legitimate businesses, which provide cover for the network's illicit activities in the region.

[218] Miryekta, "Hezbollah in the Tri-Border Area of South America."

Hezbollah's international cells constantly look for ways to innovate, through licit or illicit means. Involvement in narcotics has become an important source of funding. Hezbollah's Latin American cells have developed inputs into the narcotics trafficking pipeline moving from the TBA north through Colombia and Venezuela, which contributes to the movement of 1.5 tons of cocaine per month.[219] Outside of the TBA, Hezbollah's Latin American cells have been associated with the Colombian insurgent group the Revolutionary Armed Forces of Colombia (FARC) and their access to transnational terrorism money pipeline. Members of Hezbollah have been known to work with the Colombian cartels and the FARC to smuggle cocaine to the United States, Europe, and the Middle East. According to Colombian officials associated with the investigation: "the profits from the sales of drugs went to finance Hezbollah."[220]

3. Supportive Component

Hezbollah's Latin American cells embed into the regional Lebanese diasporas. These Lebanese diasporas appear to be located in close proximity to financially lucrative free trade zones and border crossing cities throughout the region. This facilitates money laundering and the movement of narcotics, weapons, people, and hard currency. Specifically, Hezbollah elements are embedded in the Lebanese communities of Maicao, Colombia; Margarita Island, Venezuela; Iquique, Chile; and most notably the Tri-Border region. Commonly known as the Tri-border Area (TBA), the region is an ill-governed space in South America where the borders of Paraguay, Argentina and Brazil converge. The TBA provides an environment in which terrorist cells can thrive: it provides sources of potential financing, access to illegal weapons and advanced technologies, and offers freedom of movement in a geographic area ideal for

[219] Barry LaVerle, Glenn E. Curtis, Rex A. Hudson, Nina A. Kollars, *A Global Overview of Narcotics Funded Terrorist and Other Extremist Groups*, www.loc.gov/rr/frd (accessed June 3 2010), 26.

[220] Chris Kraul and Sebastian Rotella. "Drug probe finds Hezbollah link; Officials say they've broken up Colombian ring that helped fund the militant group." Los Angeles Times, October 22, 2008, http://www.proquest.com.libproxy.nps.edu/ (accessed on June 14, 2010).

camouflage and concealment.[221] Hezbollah has invested heavily in the TBA, and has focused on the area since the early 1990s. It is likely that Hezbollah has transnational networks throughout the Lebanese diasporas in Latin America in order more efficiently move people, funds and commodities.

Hezbollah also takes advantage of the weak and corrupt governmental structures on the Colombian/Venezuelan border In Venezuela, Hezbollah works through the large Arab population on Margarita Island. The island, is a free trade zone and a known vacation destination for orthodox Muslims from around the world. Venezuelan internal security organizations were tracking a number groups or individuals associated with Hezbollah in the late 1990s and early 2000's, but those investigations have ceased since the ascendency of the Chavez regime. Margarita Island provides an operational rear-area sanctuary for Hezbollah.

Hezbollah's Latin American activities have large direct and indirect support elements. Some estimates indicate that Hezbollah receives around $10 million per month in direct support from its Iranian allies.[222] This direct support also includes the support of Iranian capacity and alliances worldwide, such as Hezbollah's Latin American cellular network. The strengthening of diplomatic relations between Iran and the Bolivarian axis of Venezuela, Bolivia, Ecuador and Nicaragua gives Hezbollah's cells a wider transnational basis of support. Historically, Iranian Embassies and cultural attaches have worked with members of the Latin American Lebanese diaspora to coordinate active support for Hezbollah operations in region.[223] Further, the deepening of relationships within the region with Iran allows for a greater facilitation of Hezbollah's freedom of movement. Travelers entering Venezuela from Iran do not have to go through immigration controls and the Morales government recently lifted all visa

[221] Randall Wood, "South America's Tri-Borders Region," *SAIS Review*, 25, No. 1, Winter-Spring 2005, 105.

[222] Karmon, *Iran and its Proxy Hezbollah*, 15.

[223] Ibid., 18.

requirements for Iranians entering Bolivia.[224] There are even reports that the Venezuelan minister of the Interior, Tarek El Aissami, was assisting in the recruitment of Venezuelans of Arab descent. He is allegedly recruiting those who were supporters of the Chavez regime in order to send them to Hezbollah training camps in Lebanon and Venezuela.[225]

Direct support activities consist of the familiar pantheon of non-lethal activities such as bribery, information operations (propaganda), and infrastructure maintenance (warehousing and safe houses). Indirect support garnered to the selective technical dark network is similar as that given to any criminal element: people, in their own self-interest, will often choose to ignore what is going on around them.

Another example of indirect support for these cells includes funding through charitable donations.[226] This type of funding is easy to produce and legitimize, and very difficult to track. Charitable giving, or Zakat, allows for unwitting support of Hezbollah's activities. Money that one might think is going to a local education establishment or support to an orphanage is bundled in a package and sent back to Hezbollah to fund the cause.

F. VULNERABILITIES AND CONCLUSION

Hezbollah's operations in the Americas are representative of a Type-III configuration. However, Hezbollah's increasingly robust activity in Latin America generates vulnerabilities due to the violations of the principles of security and resilience. These vulnerabilities come from their reliance on operatives with questionable tradecraft and a desire to maintain too much control over what should be completely decentralized and compartmented operations.

[224] Karmon, *Iran and its Proxy Hezbollah*, 20.

[225] Ibid., 21.

[226] Douglas Phillippone, *Hezbollah, the Network and Its Support Systems, Can They be Stopped?* (Monterey, CA: Naval Postgraduate School, 2008), 21.

First, Hezbollah violates the principal of security. Hezbollah's Latin American network exchanges security for agility. These cells are in a constant state of conducting ongoing support operations, while simultaneously developing operational contingency plans. Being a support and operational node simultaneously decreases security because the pre-mission activities are conducted by local operatives who possess varying abilities to utilize tradecraft, from excellent to incompetent. Through incompetency, local security agencies have interdicted Hezbollah operatives conducting pre-mission surveillance on US Embassies in Asuncion, Cyprus, Russia and Spain.[227] The loss of the operative in Asuncion, Paraguay, Sobhi Mamoud Fayad, cost the network an agent who had managed to raise $50 million.[228] This idea that all the members of the network must take part in jihad exposes those with weak operational skills to interdictions.

Furthermore, Hezbollah violates security through its reliance on the Latin American mosque network, which also sometimes functions as a control element for the network. The use of Islam to build the dark network creates an indicator through which may serve as a start point to illuminate and interdict the network. Additionally knowing that maintains Hezbollah's ties to Iranian activities, and that the Iranian regime maintains limited control over Hezbollah activities, one can watch the diplomatic activities of Iran in the region and likely be able to track the corresponding movements of Hezbollah movements. For instance, after Iran established relations with Bolivia, one could track Hezbollah activists through the establishment of new mosques in that country.[229]

Second, Hezbollah violates the principle of resilience. The network trades resilience for control and maintaining too much direct oversight on operatives who should remain dispersed. In 2008, Colombian police arrested a Lebanese crime kingpin in Bogota, named Chekry "Taliban" Harb. Harb acted as the hub of

[227] Miryekta, "Hezbollah in the Tri-Border Area of South America."

[228] Ibid.

[229] Karmon, *Iran and its Proxy Hezbollah,* 19.

an alliance between South American cocaine traffickers and Middle Eastern militants.[230] His money laundering washed hundreds of millions of dollars a year, from Panama to Hong Kong, while paying a percentage to Hezbollah. He developed a pattern due to his extensive travel to Lebanon and Syria, likely conducting meetings with his Hezbollah contacts. More recently, Hezbollah operative Jameel Nasr, who was active in the Mexican border city of Tijuana, had taken frequent trips to Lebanon and Venezuela, to receive information and instructions.[231] This travel created a profile that raised the interest of Mexican security services and invited undue scrutiny on Nasr. The Hezbollah core directors appear to be keeping very close and direct ties to their peripheral directors, which creates communication and travel patterns, which can lead to illumination. These patterns become points by which opposition forces can illuminate the network. These operatives all have specific skills that, when lost, cannot be easily replicated.

In conclusion, the vulnerabilities in of a Type-III dark network configuration have to with violations of the principals of security and resilience because of the network's desire to exert greater control. Although these Selective-Technical networks are effective in creating long duration clandestine and covert support mechanism, they are vulnerable to interdiction through the patterns they develop.

While Type-III dark networks are often auxiliary or extended support mechanisms for other networks, they are, in the pure design example, essentially autonomous entities and develop a distinct structure according to their purpose. While they tend to be aligned with a primary ideology, that does not preclude them from facilitating the activities of other dark networks to generate funds or build strategic alliances. They find sanctuary by blending into ill-governed areas

[230] Chris Kraul and Sebastian Rotella. "Drug probe finds Hezbollah link; Officials say they've broken up Colombian ring that helped fund the militant group." *Los Angeles Times*, October 22, 2008, http://www.proquest.com.libproxy.nps.edu/ (accessed on June 14, 2010).

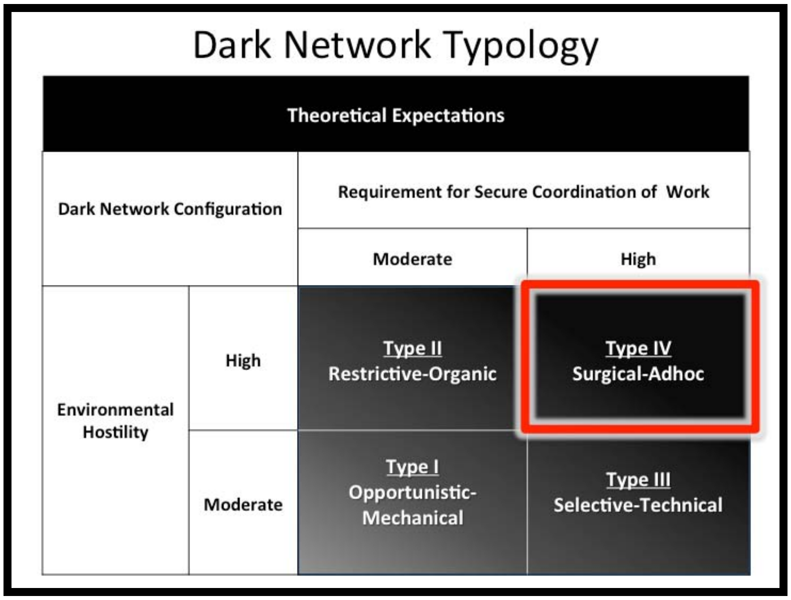
[231] Jack Khoury, "Mexico Thwarts Hezbollah Bid to set up South American Network" *Haaretz News Service,* October 29, 2010, http://www.haaretz.com/news/diplomacy-defense/mexico-thwarts-hezbollah-bid-to-set-up-south-american-network-1.300360 (accessed on November 5, 2010)

that have high levels of illicit activities, and thus are better able to conceal their activities. By inserting Hezbollah agents into Lebanese diasporas and other organized crime groups throughout the Latin America, Hezbollah has been able develop long duration networks that are able to recruit, expand, self-sustain, generate resources for the greater larger network and prepare for decisive operations when directed by the strategic core.

THIS PAGE INTENTIONALLY LEFT BLANK

VII. TYPE-IV DARK NETWORK: SURGICAL-AD HOC

A. INTRODUCTION



Dark Network Typology

Theoretical Expectations

Dark Network Configuration		Requirement for Secure Coordination of Work	
		Moderate	High
Environmental Hostility	High	Type II Restrictive-Organic	Type IV Surgical-Adhoc
	Moderate	Type I Opportunistic-Mechanical	Type III Selective-Technical

Figure 25. Type-IV Dark Network Quadrant

The purpose of this chapter is to illustrate an example of a dark network whose design state is defined by high environmental hostility and high requirements for the secure coordination of work that yields what we call the Type-IV Surgical-Ad Hoc configuration.

Type-IV dark networks can include the action cells of high-risk operations used by terrorist organizations, insurgents, and state security services. One example is the covert action team formed by the Israeli Mossad in response to the 1972 Munich Olympic Massacre. The response was initiated by the Mossad who formed several assassination teams with specific mission requirements. The teams used detailed planning, preparation, and covert communications to accomplish their objectives. Another example is the Hamburg Network, responsible for the terrorist attacks carried out on September 11.

For our illustration of a Type-IV dark network configuration, we will use the Hamburg network. We chose this dark network for our example because the network was transnational, there is a large amount of information and data available, and it most closely illustrates the typological design state of a Type-IV dark network.

B. OVERVIEW OF THE HAMBURG NETWORK

The Hamburg Network was a group of 24 radical Islamists operating in five cells and responsible for the 9/11 terrorist attacks. The origins of the network lay with a study group at al-Quds Mosque in Hamburg, led by Mohammad Belfas.[232] The group originally consisted of Mohamed Atta, Mounir Motassadeq, and Abdelghani Mzoudi who were all studying at the Technical University of Hamburg-Harburg (TUHH). Over time, the study group grew to include Ramzi bin al-Shibh, Said Bahaji, Zaid Amir Jarrah, Zakarya Essabar and Marwan al-Shehhi. The actual "Hamburg Contingent" began out of this study group when Mohammed Atta, Ramzi bin al-Shibh, and Said Bahaji moved into an apartment together on 53 Marienstrasse, which they named "Bait al-Ansar" or "the House of the Supporters (of the Prophet)."[233] It was there that the three held meetings to discuss their anti-American and anti-Israeli views and began trying to find ways to further their cause.[234] With all eight associated through the study group led by Belfas and their increased social interaction through school, meetings, and weddings, their discussions grew more "virulent" and ultimately led to the friends

[232] Sageman, *Understanding Terror Networks*, 103-104.

[233] The individuals that met in the study group in Hamburg are widely known as the Hamburg Cell. This thesis will use the 9/11 commission report identifying them as the Hamburg Contingent who became part of the larger Hamburg Network. See National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report*, http://www.gpoaccess.gov/911/index.html (accessed on November 17, 2010).

[234] Sageman, *Understanding Terror Networks,* 105.

looking to join the jihad and go to Chechnya to fight the Russians. It was not until they met Mohamadou Ould Slahi who encouraged them to travel to Afghanistan for training.[235]

Prior to, and completely independent of the forming of the Hamburg Contingent, the plan for the "planes operation" was developing in the mind of Khalid Sheikh Mohammed (KSM). KSM knew that his plan for using airplanes in a terrorist attack on the United States required personnel, money, and logistical support that he did not have, but Usama bin Ladin did. KSM knew he had to meet with bin Ladin because of he could provide the personnel, money, and logistical support required. KSM formally joined Usama bin Ladin and al-Qa'ida in 1998 after being given the green light for his "planes operation."[236]

With the arrival of the first three members of the Hamburg Contingent in Afghanistan, Usama bin Ladin was about to find the perfect group to lead the attack: the members of the Hamburg Contingent spoke fluent English, were educated and knowledgeable of the western lifestyle, and were radical Islamists. In November of 1999, Mohamed Atta and his Hamburg Contingent became the strategic core of the dark network responsible for the 9/11 attacks.[237]

C. TYPE IV DESIGN STATE

1. High Hostility of the Environment

This configuration results from a design state with high level of hostility in the environment. The high level of hostility is typically due to a sophisticated "enemy", such as the government of a nation-state with a well-resourced security

[235] Sageman, *Understanding Terror Networks,* 106.

[236] Khalid Sheikh Mohammed did not join Usama bin Ladin and Al-Qa'ida when originally invited in 1996 because he wanted to remain independent. This allowed him to remain free to work with other organizations, such as the mujahideen led by Sayyaf, Sheikh Mohammed's mentor, who was loyal to Massoud, the leader of the Northern Alliance. Since bin Ladin was forging ties with the Taliban, the opposition of the Northern Alliance, allying with Al-Qa'ida would have proven troublesome for Sheikh Mohammed. See National Commission on Terrorist Attacks Upon the United States, "Al-Qa'ida Aims At The American Homeland", http://www.9-11 commission.gov/report/911Report_Ch5.htm (accessed on August 30, 2010).

[237] Sageman, *Understanding Terror Networks,* 106–107.

apparatus, such as the Central Intelligence Agency (CIA) or Federal Bureau of Investigation (FBI). The environmental hostility level can also be attributed to the nature of the population. If the population is against the purpose of the network, then the hostility is high.

While it may not seem so at first glance, the Hamburg Network operated in an environment with a high level of hostility. The environmental hostility in Hamburg was high because German security forces were monitoring them for their affiliation with known nodes of Islamist activity. So, the Atta's network ensured that their activities did not warrant any further attention or investigation. According to the 9/11 Commission, the Hamburg network changed their appearance to better fit with the Western society and they distanced themselves from Islamist nodes.[238] Adoption of clandestine and covert behavior permitted the Hamburg Network to survive in a hostile environment and hide in plain sight.

Hostility is the United States was also high, but the Hamburg network identified and exploited vulnerabilities in U.S. security apparatus to remain hidden and achieve its purpose. Security measures, specifically with respect to aviation, were lackadaisical. Passenger and baggage screening was not introduced until 1972 and was generally contracted to private security companies and oversight of the security measures was held by the Federal Aviation Administration.[239] The airport security measures were also "hampered" by those who felt changes in procedures were discriminatory in nature.[240] The lackadaisical security measures also existed within customs and immigration. According to the 9/11 Commission, "before 9/11, security concerns were not a major factor in visa issuance unless the applicant already was on a terrorist

[238] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report*.

[239] National Research Council Committee on Commercial Aviation Security, *Airline Passenger Security Screening: New Technologies and Implementation Issues*, (Washington D.C.: National Academy Press, 1996), 6.

[240] "FAA enacts new airport security measures," *CNN Travel* (January 2, 1998), http://articles.cnn.com/1998-01-02/tracel/9801_02_airline.safety_1_air-passenger-screening-security-measures-new-rules?_s=PM:TRAVEL (accessed on December 1, 2010).

watch list."[241] Because of these shortcomings in security and the fact that the selected 911 hijackers were not on a watch list, the dark network remained undetected had freedom of movement in both Hamburg and the United States.

2. High Requirement for Secure Coordination of Work

The high hostility in the environment also lends itself towards the high requirement for the secure coordination of work. A Type-IV dark network is unable to operate openly for risk of detection and detention. The high requirement for secure coordination of work results in more detailed planning, compartmentalization, use of coded transmissions, deception operations, and highly effective tradecraft in order to hide or mask activities.

The Hamburg Network conducted varying degrees of clandestine and covert behavior activity to meet the high requirement for secure coordination of work. In order to prevent compromise of the "planes operation", the Hamburg network began distancing themselves from extremists, wearing western clothing, and even shaved their beards.[242] The change in appearance also helped them during international travel. Atta believed "that if the hijackers were clean shaven and well dressed, others would think them wealthy Saudis and give them less notice."[243] Some of the network members claimed they lost their passports and obtained new ones before applying for visas to enter the United States. This was done to cover their previous travel to Afghanistan.[244] It was through the secure coordination of work via covert and clandestine activity that the Hamburg Network was able to go relatively unnoticed by German and U.S. authorities.

[241] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report*, 168.

[242] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report*, 167–168.

[243] Ibid., 245.

[244] Ibid., 168.

D. TYPE-IV DARK NETWORK: SURGICAL–AD HOC

We characterize Type-IV dark networks as surgical and ad hoc for the following reasons.

1. Surgical Action

The activity of a Type-IV dark network is surgical in nature due to the high environmental hostility and the specificity of the intended action. Planning must be precise and communications must be concealed. These networks rely on a high level of clandestine and covert tradecraft to mask their true nature and identity in an effort to avoid detection. For the Type-IV dark network to accomplish its purpose, it must be able to recruit candidates, properly vet and indoctrinate them, and train them, while avoiding detection. Given the requirement for members to conduct pre-execution activities without being detected, the network must design itself to incorporate elaborate security measures to coordinate work and prevent catastrophic destruction. Because of this, operational planning and preparation could take years.

2. Ad Hoc Configuration

According to Mintzberg, an adhocracy is a sophisticated configuration where the network is created "from different specialties into smoothly functioning project teams."[245] There are two types of adhocracy: operating and administrative. An operating adhocracy serves a client and an administrative adhocracy serves the organization, or network, itself. In design terms, an adhocracy is a configuration with little formalization of behavior, horizontal job specialization based on formal training, a grouping of professional specialists in functional units, a reliance on a "liaison" to allow for mutual adjustment both within and between the units and finally a selective decentralization to the units which are located at various places in the organizations.[246] Additionally,

[245] Mintzberg, "Structure in 5's," 336–337.

[246] Ibid., 336–337.

members of an ad hoc network tend to be young.[247] This fresh perspective and autonomy gives the ad hoc configuration agility and resiliency. From the perspective of dark networks, an ad hoc configuration enhances security by providing cells an inherent multifunctional capacity to achieve its purpose. This inherent capacity reduces the need for external connections and increases compartmentalization, thus increasing security.

E. FUNDAMENTAL COMPONENTS

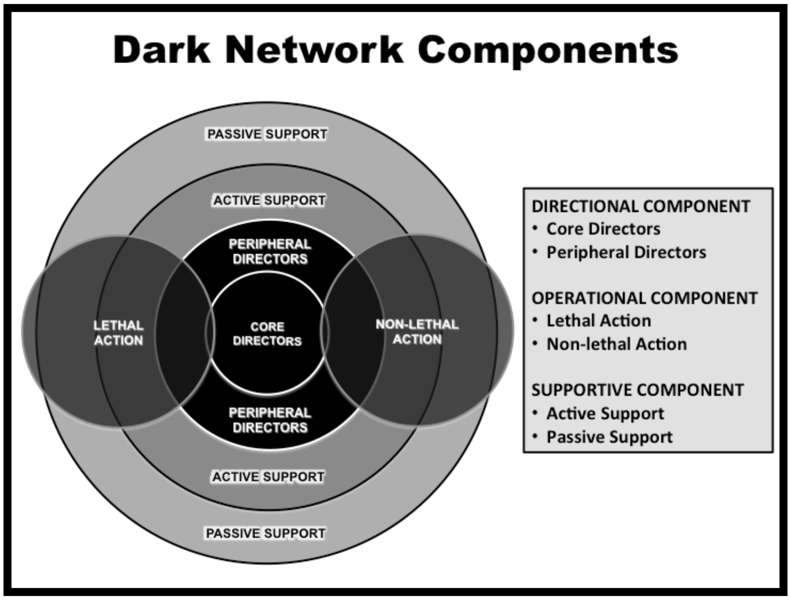


Figure 26. Illustration of Dark Network Components

1. Directional Component

The Hamburg Network began as a student study group at a mosque in Hamburg, Germany. The core members of the group were Mohammed Atta, Ramzi Binashibh, Marwan al Shehhi, and Ziad Jarrah.[248] Their initial direction came from their “instructor,” Mohammad Belfas, who played an informal leadership role. As the radical interests of the members grew, they began to

[247] Ibid., 338. replace and format

[248] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report*, 160–165.

discuss plans and/or ways in which to further their cause, ultimately choosing to join the jihad. The group was young and willing to be trained in specialized tasks. Influenced by an individual with more time and connections to the Islamist movement and the jihad, they traveled to Afghanistan for paramilitary training. While there, they were identified as having all the skills and traits to execute a plan already being developed by Usama bin Ladin and Khalid Sheikh Mohammed. Once at this stage, strategic direction came from the larger organization of al-Qa'ida, namely Usama bin Ladin, and became the Hamburg Network. In this sense, the Hamburg Network was an administrative adhocracy, with bin Ladin and Sheikh Mohammed forming the strategic core. Within the cell, Mohamed Atta was the key player for operational planning and with the remaining actors of the cell, became a peripheral director responsible for executing the "planes operation." Together they operationalized the strategic ideology of the al-Qa'ida movement to achieve the network's purpose: strike the infidel. It was through the "sponsorship" of al-Qa'ida's core directors that the Hamburg Cell was able to carry out the operation designed by KSM. Since this was a surgical–ad hoc dark network, day-to-day operations did not require a separate strategic ideology that differed from that of the global Salafi jihad. Therefore, the key actors of the Hamburg Network—namely, Atta, al-Shehhi, Jarrah, and later Hanjour—filled the roles of both core and peripheral directors for the execution of the 9/11 attacks.

2. Operational Component

The surgical nature of this network meant it was designed for a very specific task and the operational component of this dark network did exactly that. Within its operational component, the Hamburg Network conducted primarily lethal decisive action through the actions of the hijackers. They physically took over the aircraft, killing crew members in the process, in order to use them as the weapons to destroy their targets. The next example of lethal decisive action is easy to identify: the aircraft striking the World Trade Center towers and the Pentagon. They failed to strike their suspected 4th target, the U.S. Capitol. The precision of planning within the operational component was also in line with the surgical nature of the network. For example, at some point each hijacker travelled first class on an east-west transcontinental flight on the same type of aircraft he would be piloting on September 11. This planning continued in their ability to use banks within the United States to obtain the money used in their attacks. According to the 9/11 Commission Report, "all of the hijackers opened accounts in their own name, and used passports and other identification documents that appeared valid."[249] While they were not experts, their careful planning allowed them to set up their access to financing.[250] Further examples of the precise planning within the operational component, ranging from the research of flight schools to practice flights down the Hudson River corridor, are presented in the 9/11 Commission Report.

Operational security of the Hamburg Network was a combination of compartmentalization, tradecraft, and the use of cut-outs. The secure coordination and synchronization of output to achieve ideological objectives was achieved by the utilization of ties. As a surgical-ad hoc dark network, the Hamburg Cell did not form new ties outside of the network without proper "vetting" or introductions (existing members, mentors, established al-Qa'ida members, Usama bin Ladin, and Khalid Sheikh Mohammad appear to be the only people who introduced new ties to the network). Also, they minimized ties within the network through compartmentalization. Meetings were held with the use of cross-ties to "connect distant parts of the network to coordinate tasks and report progress." Following the meetings, these cross-ties would go dormant.[251]

The network was surprisingly sparse and many of the actors within the same team were very "distant" from each other. According to Krebs, "many pairs of team members [were] beyond the horizon of observability from each

[249] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report*, 242.format all of these – not indented correctly

[250] Ibid., 237.

[251] Krebs, "Mapping Networks of Terrorist Cells," 46–47.

other…keeping cell members distant from each other, and from other cells."[252] This distance minimizes the possible damage resulting from the kill, capture or compromise of any single cell member. Usama bin Ladin claimed "those who were trained to fly didn't know the others. One group of people did not know the other group."[253] The Hamburg Network was less able to adapt to changes in the environment due to the incredibly covert nature of their group and its operation. Direct and open communication between the members and their "leaders" was not possible. They were already highly covert and "living in plain sight" which did not allow for much flexibility due to the risk of detection. The Hamburg Network was resilient in the fact that its compromise would not cause the disintegration of their sponsor, al-Qa'ida, nor would it adversely impact the greater global Salafi jihad. However, interdiction of the Hamburg Network itself would not have been survivable.

3. Supportive Component

The Hamburg Network had both active and passive support components. Because of the highly covert nature of the network, the flight instructors constitute active support. While there were no obvious indicators to lead the flight instructors to suspect their students intended to use their knew skills in a terrorist plot, the instructors still played an active support role, albeit unwitting. This was partly possible due to another unwitting active support component, the U.S. Customs and Immigration office. In February 2000, Atta and the other members chosen to be pilots for the attack claimed their passports were stolen and obtained new passports in order to cover incriminating stamps. This allowed them to contact flight schools in the United States to obtain visas to enter the

[252] Ibid., 46.

[253] United States Department of Defense, Transcript of bin Ladin Video Tape, December 13, 2001, http://www.defenselink.mil/news/Dec2001/d20011213ubl.pdf (accessed November 11, 2010).

country.[254] Also included in the supportive component is the network's ability to sustain its capacity to produce output. Until taking the advice of Mohamadou Ould Slahi to go to Afghanistan for training, the group had minimal capacity. They were radicalized, but did not have the means to produce output. They needed to *join* a jihad versus developing operations on their own. Once they went to Afghanistan, they joined the greater cause of al-Qa'ida. Their capacity to produce output was tied to this association. The effort of the Hamburg Network was sustained by its association with Usama bin Ladin and through the logistical system (money and personnel) made available. While there were nineteen total hijackers, there were multiple other accomplices who never got on an airplane. Individuals responsible for money, logistics, skill training at the terrorist training camps in Afghanistan—all are part of the active support component.

Passive support components include the law enforcement agencies, schools and mosques that allowed the collusion of the members. German law enforcement officials were watching the cell members, known to be radicalized students, who shared an apartment, knew they and others who visited attended a "study" group at the al-Quds Mosque in Hamburg, yet they did not share the information with other intelligence agencies.[255] Long-term sustainability of an adhocracy has many unknowns. As previously stated, an adhocracy does not know where or when its next job will come. It can easily be overcome by operational tempo (OPTEMPO) without a capable internal or external logistical system.

F. VULNERABILITIES AND CONCLUSION

While the Hamburg Network is presented as an example of the ideal configuration of a Type-IV dark network, there are still vulnerabilities where the

[254] Peter Finn, "Hamburg's Cauldron of Terror," *The Washington Post* (online), September 11, 2002, http://www.washingtonpost.com/ac2/wp-dyn/A64793-2002Sep10?lan (accessed November 2, 2010).

[255] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report*.

design type does not adequately follow the principles of design. The Hamburg Network is vulnerable in the areas of security, agility, resilience and capacity. It is also vulnerable due to the surgical nature of its operation.

First, it is vulnerable based on the principles of security and agility. Covert networks trade efficiency for secrecy. However, they have to coordinate through task-based communication. It is during these periods of communication that they are vulnerable. The Hamburg Network takes a seemingly calculated risk on the principle of security to ensure effective communications for control and direction setting. Second, the network has cross-ties or transitory short-cuts[256] that coordinate tasks and report on progress. While the network as a whole may be compartmentalized, the actors who serve as cross-ties have more knowledge of the overall organization of the network. Remove these actors, and task-based coordination cannot occur effectively and can uncover and/or foil the operation. Third, it is vulnerable on the principle of resilience. Most adhocracies are young and its members have a tendency to die young or move on (as previously mentioned). They never know where their next job will come from which could lead those on the periphery to shift to another type of network for greater stability or to fill their desire to be a bigger part of the cause.

An additional vulnerability stems from the surgical aspect of this configuration. A surgical operation requires specific skill sets. As demonstrated by the Hamburg Network, internal ties tend to be most concentrated around the unique skill sets. According to Krebs, “concentrating both unique skills and connectivity in the same nodes makes the network easier to disrupt.”[257]

Finally, this configuration type is highly susceptible to misinformation and deception. Due to the highly compartmented nature of the network, many do not know each other. Planting seeds of mistrust within the network can lead

[256] According to Valdis Krebs, the “judicious” use of transitory short-cuts connect distant parts of a network to coordinate tasks and report progress. See Krebs, “Mapping Networks of Terrorist Cells.”

[257] Ibid., 50.

members of the network to doubt the overall direction of the network, which in turn could lead to defection from the network or possibly lead members to go to authorities and report on those they think may be reporting on them.

This section illustrated the Type IV Dark Network Configuration: Surgical–Ad Hoc through the depiction of the Hamburg Network. The high level of environmental hostility does not allow for much freedom of movement, therefore the surgical action and ad hoc configuration of this type of dark network require precise planning, clandestine and covert communications, and compartmentalization for the accomplishment of the network’s purpose. Because the Hamburg Network conducted tradecraft associated with clandestine and covert behavior, the network successfully avoided illumination and interdiction and achieved its purpose in an environment with a high level of hostility.

THIS PAGE INTENTIONALLY LEFT BLANK

VIII. CONCLUSIONS AND RECOMMENDATIONS

A. A THEORY OF DARK NETWORK DESIGN

We have defined dark networks as interdependent entities that use formal and informal ties to conduct licit or illicit activities and employ operational security measures and/or clandestine tradecraft techniques through varying degrees of overt, or more likely covert, activity to achieve their purpose. Dark networks have natural configurations and that these configurations vary according to the network's purpose and design state. While no two networks are exactly alike, they have similar basic components that are configured to produce output through coordinated work in order to achieve a purpose. Each dark network design, based on design state, configures itself through the arrangement of three fundamental components: directional, operational, and supportive.

The design state is determined by two dimensions: hostility of the environment and the requirement for the secure coordination of work. From these dimensions, we presented the four dark network configurations or designs: Type-I: Opportunistic-Mechanical; Type-II: Restrictive-Organic; Type-III: Selective-Technical; and Type-IV: Surgical-Ad Hoc. The four dark networks presented in this study—Mara Salavatrucha 13, Provisional Irish Republican Army, Hezbollah in Latin America, and the Hamburg Network—offer illustrative examples of our four dark network configurations. By illustrating the four dark network design types, we were able to present basic vulnerabilities of each after analyzing them using the six principles of dark network design: security, agility, resilience, direction setting, control, and capacity. To the extent a dark network is not configured to address the level of hostility in its environment, or the requirement for secure coordination of work by adhering to the principles of dark network design, it becomes vulnerable to illumination and interdiction.

1. Environmental Hostility

A dark network must configure itself to survive in the face of hostility. Hostility ranges from low to high, as presented in Chapter II. While dark networks typically operate in a highly hostile environment, which in turn requires the network to employ strict security measures, some modern dark networks operate throughout the continuum. In the four dark network configuration types presented in this research, the level of environmental hostility varied. Type-I and Type-III operate in a moderate level of environmental hostility while Type-II and Type-IV operate in a high level of environmental hostility.

a. Moderate Hostility

In the case of the Type-I Opportunistic-Mechanical dark network, the moderate level of hostility in the environment is the result of the limitations of the state. The dark network is aware that the state can (and will) only use a limited application of force to inhibit their efforts. In the case of the Type-III Selective-Technical dark network, the moderate level of hostility is the result of their location, perhaps an ungoverned space or they may have the support of the population. This typically provides freedom of movement and action for the network.

b. High Hostility

The Type-II Restrictive-Organic dark network is configured for high levels of environmental hostility. The high level of hostility typically results from the network being in opposition to the governing state. The Type-IV Surgical-Ad Hoc dark network is configured for the highest level of environmental hostility. It must configure to protect itself from constant risk of detection and attack as it is always being hunted.

2. Secure Coordination of Work

The secure coordination of work required by a dark network refers to its need and desire to commit resources in a way to achieve objectives without detection and possible destruction. The secure coordination of work permeates the dark network, enabling coordination between the directional, operational, and supportive components of the dark network to achieve its purpose. The requirement for secure coordination of work is not always dependant on the level of hostility in the environment. Type-I and Type-II dark networks have a moderate requirement for the secure coordination of work and Type-III and Type-IV dark networks have a high requirement.

a. Moderate Requirement for Secure Coordination of Work

Despite the moderate level of hostility in the environment for the Type-I dark network, some amount of secure coordination is required for the accomplishment of purpose. Regardless of the freedom of movement enjoyed by the network, it cannot survive if its operations and coordination are broadcast openly. In the case of the Type-II dark network, the level of hostility in the environment is high, but the high level of support from the surrounding community allows for a liberal freedom of movement which in turn allows for moderate levels of secure coordination of work. This type of network can maintain both a clandestine and covert lifestyle, emerge to conduct an act, and then return underground when threatened. It thrives off the security provided by the support of the population. As illustrated by Hezbollah in Latin America, support from the population, despite being considered a terrorist organization on the national stage allows for a tremendous amount of success.

b. High Requirement for Secure Coordination of Work

Both the Type-III and Type-IV dark networks require high levels of secure coordination of work. With the Type-II dark network, while it enjoys freedom of movement due to its operations from a sanctuary or supportive population, its activities are highly illegal (smuggling, illegal financing, etc) and business cannot be conducted openly for risk of detection. For a Type-IV dark network, the high level of environmental hostility and highly compartmented nature of the network naturally lend itself to the requirement of highly compartmented and secure coordination of work. As demonstrated by the Hamburg Network, ensuring all members did not have complete knowledge of the plan or complete knowledge of the membership of the cell conducting the operation protected it from the multiple set-backs that would have disrupted their plan had they been configured differently.

3. Adherence to the Principles of Dark Network Design

We show that regardless of design state, there are fundamental challenges that all dark networks must address. From our two stated design dimensions as well as the body of literature examined in Chapter II, we identified six design challenges which we present as the principles of dark network design: security, agility, resilience, direction setting, control, and capacity. Through our illustrative examples of each typological configuration, we have shown how each dark network addressed the six principles. In the figure below, we present our findings based on the illustrative examples and whether they adequately addressed each principle of dark network design.

Table 2. Network Adherence to Principles of Dark Network Design

	MS-13	**PIRA**	**HEZBOLLAH**	**HAMBURG**
Security	NO	NO	NO	YES
Agility	NO	NO	YES	NO
Resilience	NO	YES	NO	NO
Direction Setting	YES	YES	YES	YES
Control	YES	YES	YES	YES
Capacity	NO	YES	YES	NO

While we did not make a specific indication of success or failure, we submit that failure to adhere to these six principles can have potentially fatal consequences. It is through the examination of each dark network typological configuration with respect to these design principles that we can identify potential vulnerabilities and provide possible recommendations for illumination and interdiction of the dark network.

B. INSIGHTS FROM OUR RESEARCH

Over the course of developing our theory of dark network design and analyzing our four illustrative examples, some insights emerged. First, networks are dynamic and will evolve over time. The environment in which these networks operate is not static; therefore in order to survive the networks must adapt to fit the environment. Additionally, throughout the life cycle of the network, if it is successful, it will continue to grow. According to Jones, cellular networks will "grow purposefully" and "as they grow, the leadership of the network decentralizes tactical decisions, but maintains operational and strategic control."[258] However, our study, as well as organizational design theory, further suggests that as a network grows and faces environmental hostility, it will tend to become more centralized in an effort to exert more control. "To deal with crises, organizations tend to centralize at the top temporarily, and to suspend their standard operating procedures."[259]

Second, there is a balance that must be achieved both within and outside of the network in order for it to survive. With respect to the principles of dark network design, going to far in any one direction on one principle can result in the sacrifice of another. Simply put, the overemphasis of one results in the detriment of another. Pushing a network out of balance can create a vicious cycle leading to network failure. For example, if the environmental hostility is increased on a Type-I dark network, it may be forced to exert more control and become more centralized. In becoming more centralized, the network then becomes less resilient and agile and may develop security vulnerabilities. If we can keep the

[258] Jones, *Understanding the Form, Function, and Logic of Clandestine Cellular Networks*, 30.

[259] Mintzberg, "Structure in 5's," 332.

dark network off balance and continue to push it towards a boundary, we can induce a vicious cycle leading to failure of the dark network.

Keeping in mind the principles of dark network design as well as the insight that networks are dynamic and can be pushed out of balance, we can suppose possible strategies for illumination and interdiction of a dark network.

C. RECOMMENDATIONS FOR ILLUMINATION AND INTERDICTION

1. Understand and Change the Environment

In the examples presented for each type of dark network configuration, the importance of the environment on that configuration is critical. Understanding the environment that the network has configured itself to maximize operations within and then changing it to make that configuration a mismatch will affect the mode of operation and/or the methods of communication and potentially illuminate the network. In the case of a Type I dark network, which is most likely a known and visible illegal entity, but operating freely due to the lack of effective response from the state, changing the environment applies as well. Looking at MS-13, one can observe that they operate freely as a result of law enforcement system that is neither networked nor coordinated and generally limited in its response capabilities. Change that factor of the environment and MS-13's configuration will be a mismatch, exposing it for more effective interdiction.

2. Exploit External and Internal Network Misalignment

While the dark networks presented in the illustrative examples depict network configurations that are suited to achieve their purpose in their defined design state, opportunities exist to create or exploit vulnerabilities that make the networks susceptible to illumination and interdiction. Most are neither perfectly designed to fit the environment, nor are they likely to continuously and strictly adhere to the necessary levels of secure coordination of work. Put quite simply: everyone slips up at some point. For this reason, each network configuration provides opportunities for exploitation.

A dark network is misaligned with the external environment when its purpose and design are diametrically opposed to the optimum design state. Strategies designed to increase uncertainty in the external environment, thus increasing hostility, forces the network to redesign to fit its changing environment. If the network lacks agility and is slow to adapt to its changing environment, then it is susceptible to illumination and interdiction. If a nation-state or other legitimate authority increases its will and capacity to combat dark networks, then the dark networks become misaligned with their environment and have three basic options: reconcile, stay and fight, or run and hide. Mitigating the antecedent conditions that enable dark networks to operate creates conditions that are unfavorable to achieve their desired purpose. Removing the causal factors that push people into dark networks drastically reduces the places to hide, the network's sources of ideological, personnel, and material support, and influences reconciliation. Creating a caustic environment for the dark network allows legitimate authorities to focus their resources on illuminating and interdicting the remaining hard-core entities of the dark network.

As previously explained, clandestine networks trade efficiency for secrecy, or vice versa. Strategies that cause internal misalignment within the dark network reduce the network's capacity for secure coordination of work to achieve its purpose. We submit the following framework to generate internal vulnerabilities in dark networks: cause confusion, friction, gridlock, internal competition, and low performance with interdiction strategies that cause misalignments of the dark network's strategy, structure, processes and lateral capability, rewards systems, and people practices. The resulting internal misalignment decreases the capacity for secure communication and coordination, which directly impacts the efficiency of a dark network. In the case of the Provisional Irish Republican Army (PIRA), communications and coordination in a hostile environment was a problem. In order to communicate, messengers and dead drops were utilized and one poorly worded note could lead to misunderstanding and in-turn lead to failure of an intended mission.

Interjecting unclear, misguided, and false information into the communications of a dark network can further destroy efficiency leading to them resort to more overt communications and therefore illuminating the network.

3. Develop Dark Counter-Networks

It is critical to have the capacity to identify, understand, and defeat dark networks that pose a threat to U.S. national security. Simply put, dark networks can be a tools for fighting opposition dark networks.

D. RECOMMENDATIONS FOR FURTHER STUDY

This study had most likely generated more questions than it has answered due to the complexity of the subject. For this reason, we hope it will serve as a catalyst for further research. We offer the following recommendations for further study based on dark network design:

1. Use of Geospatial, Temporal, and Network Analysis Tools

Test aspects of our theory of dark network design using visual analytic tools to explore the geospatial, temporal, and network aspects of dark, light/bright, and gray networks. These tools are useful for not only tracking and disrupting opposition dark networks, but also aid in modeling and testing the integrity of sanctioned dark networks.

2. Deep-Dive Each Design State

Conduct an in-depth case study comparison on dark networks within the same design state measured against concepts presented in our theory of dark network design to find common characteristics in their configurations. Subsequently, compare and contrast the common characteristics of each design state to determine correlations among the different components and sub-component of dark networks as outlined in our models.

3. Research Gray Networks as Problems

Conduct further research on gray networks as problems. Gray networks appear to operate across a broader operational continuum and with a higher degree of complexity. Their domain provides the setting that causes people to convert from passive to active support. Gaining a better understanding of this domain can aid in developing strategies that are preemptive in nature to inhibit dark networks from metastasizing.

4. Examine Unrestricted Dark Network Warfare

Apply our theory of dark network design to develop and protect sanctioned dark networks to counter opposition dark networks and opposition nation-states that are a threat to U.S. national security. Develop concepts for conducting unrestricted dark network warfare. Based on the current state of the security environment, we posit that the networked-form of asymmetric clandestine and covert warfare between state and non-state actors will be the prevalent mode of conflict for the rest of the century. With that in mind, we re-emphasize our core finding that “dark networks matter.”

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Adams, James. *The Financing of Terror*, New York: Simon and Shuster, 1986.

al-Alwaki, Anwar. "44 Ways to Support the Jihad." *The Force of Reason*. (November 2009). Accessed June 2, 2010. http://theforceofreason.com/wp-content/uploads/2009/11/44-Ways-to-Support-Jihad.pdf.

Anklam, Patti. *Net Work: A Practical Guide to Creating and Sustaining Networks at Work and in the World*. Burlington: Elsevier, 2007.

Arpoova, Shah. “The Mullah, the Caudillo, and the Terrorist.” *The American: The Journal of the American Enterprise Institute.* 1 April 2009. Accessed on June 7, 2010. http://american.com.

Arquilla, John. "It Takes a Network: On Countering Terrorism." United States House of Representatives. (September 18, 2008). Accessed October 20, 2010. http://armedservices.house.gov/pdfs/TUTC091808/Arquilla_Testimony091808.pdf.

Arquilla, John, and David Ronfeldt. "RAND Monograph Reports - Networks and Netwars: The Future of Terror, Crime, and Militancy." RAND Corporation, 2001. Accessed on November 5, 2010. http://www.rand.org/pubs/monograph_reports/MR1382/.

———. "RAND Monograph Reports: The Advent of Netwar." RAND Corporation, 1996. Accessed on November 5, 2009. http://www.rand.org/pubs/monograph_reports/MR789/.

Azani, Eitan. *Hezbollah: The Story of the Party of God.* New York: Palgrave Macmillan, 2009.

Beam, Louis. “Leaderless Resistance.” The Seditionist, 12 (February 1992). Accessed on August 4, 2010. http://www.louis-beam.com/leaderless.htm.

Belasco, Amy. "The Cost of Iraq, Afghanistan, and other Global War on Terror Operations since 9/11." Vers. 7-5700. Congressional Research Service. September 28, 2009. Accessed on June 28, 2010. https://www.hsdl.org.

Bell, J. Bowyer. "Aspects of the Dragonworld: Covert Communication and the Rebel Ecosystem." *Journal of International Intelligence and Counterintelligence* 3, no. 1 (1989): 15–43.

———. “Dragonworld (II) Deception, Tradecraft and the Provisional IRA,” *International Journal of Intelligence and Counterintelligence* 8, No. 1 (1995), 25–50.

———. *The Secret Army*: *The IRA Rev 3rd Ed.,* New Brunswick: Transaction Publishers, 1997.

Borgatti, Stephen P., Ajay Mehra, Daniel J. Brass, and Giuseppe Labianca. "Network Analysis in the Social Sciences." *Science* 323, no. 5916 (February 2009): 892–895.

Borgatti, Stephen P., and Daniel S. Halgin. "Analyzing Affiliation Networks." In *The Sage Handbook of Social Network Analysis*, edited by Peter Carrington and John Scott. Essex: SAGE Publications Ltd, 2004. Accessed November 5, 2009. http://www.steveborgatti.com/publications/bhaffiliations.pdf.

Borgatti, Stephen P., and Pacey C. Foster. "The Network Paradigm in Organizational Research: A Review and Topology." *Journal of Manangement* 29, no. 3 (2003): 991–1013.

Borgatti, Stephen P., and Xun Li. "On Social Network Analysis in a Supply Chain Context." *Journal of Supply Chain Management* 45, no. 2 (2009): 5–22.

Brafman, Ori, and Rod A. Beckstrom. *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations*. New York: Penguin Group, 2006.

Burt, Ronald S. Structural Holes: The Social Structure of Competition. Cambridge: Harvard University Press, 1992.

Burton, Fred. “Mara Salvatrucha: The New Face of Organized Crime?” Accessed on August 11, 2010. http://www.stratfor.com/memberships/48568/mara_salvatrucha_new_face_organized_crime?ip_auth_redirect=1.

Bush, George W. Executive Order 13224 - Blocking Property and Prohibiting Transactions with Persons Who Commit, Threaten to Commit, or Support Terrorism. The White House. Washington, DC: Government Printing Office, September 23, 2001.

Caribbean Financial Action Task Force. "Money Laundering Prevention Guidelines for CFATF Member Governments, Free Trade Zone Authorities, and Merchants." The Caribbean Financial Action Task Force. 2001. Accessed June 2, 2010. http://www.cfatf-gafic.org/downloadables/doc/FTZ%20Recom.%20final-March%202001%20_En_.pdf.

Carley, Kathleen M., Ju-Sung Lee, and David Krackhardt. "Destabilizing Networks." *Connections* 24, no. 3 (2001): 31–34.

Carlile, Michael K. Into the Abyss: A Personal Journey into the World of Street Gangs. April 7, 2010. Accessed November 5, 2010. http://people.missouristate.edu/MichaelCarlie/.

Castells, Manuel. "Afterward: Why Networks Matter." in *Network Logic: Who Governs in an Interconnected World?*, edited by Helen McCarthy, Paul Miller and Paul Skidmore, 221–225. London: Demos, 2004.

———. *The Rise of the Network Society*. Cambridge: Blackwell Publishers, 1996.

Cline, Lawrence E. "Pseudo Operations and Counterinsurgency: Lessons from other Countries." United States Army War College Strategic Studies Institute. June 2005. Accessed November 8, 2009. http://www.carlisle.army.mil/ssi/pubs/display.cfm?PubID=607.

Commonwealth of Virginia Department of State Police Virginia Fusion Center. "Mara Salvatrucha 13 (MS-13) Intelligence Report," July 2008. Accessed on November 15, 2010. http://info.publicintelligence.net/VFCMaraSalvatrucha.pdf.

Coogan, Tim Pat. *The IRA*, London: Harper Collins, 2000.

Covin, Jeffrey G., and Dennis P. Slevin. "Strategic Management of Small Firms in Hostile and Benign Environments." *Strategic Management Journal* 10 (1989): 75–87.

Curtis, Glenn, and Tara Karacan. *The Nexus Among Terrorists, Narcotics Traffickers, Weapons Proliferators, and Organized Crime Networks in Western Europe*. Ferderal Research Division, Library of Congress. Washington, DC: Government Printing Office, December 2002.

Daft, Richard L. *Essentials of Organization Theory and Design*. 8th Edition. Madison: South-Western Educational Publishing, 2003.

Daoust, Daniel C. and Joseph E. Osborne. “Counter-Organization Targeting: A Theoretical Framework for Analysis.” Master's Thesis, Naval Postgraduate School, 1996.

de Nooy, Wouter, Andrej Mrvar, and Vladimir Batagelj. *Exploratory Social Network Analysis with Pajek*. Cambridge: Cambridge University Press, 2005.

Department of Defense. *Department of Defense Dictionary of Military and Associated Terms*. April 2010. Accessed on October 26, 2010. http://www.dtic.mil/doctrine/dod_dictionary/.

———. "Irregular Warfare: Countering Irregular Threats." Vers. 2.0. United States Joint Forces Command Joint Operating Concepts. May 17, 2010. ACCESSED JUNE 22, 2010. http://www.dtic.mil/futurejointwarfare/concepts/iw_joc2_0.pdf.

Embassy of El Salvador, “The Peace Accords.” Accessed October 23, 2010. http://www.elsalvador.org/embajadas/eeuu/home.nsf/politics.

Everton, Sean F. *Tracking, Destabilizing, and Disrupting Dark Networks Using Social Network Analysis*. Monterey, CA: Naval Postgraduate School, 2009.

The Federal Bureau of Investigation. “The MS-13 Threat: A National Threat Assessment.” Accessed on August 11, 2010.

Felix, Christopher*. A Short Course in the Secret War*. New York: Madison Books, 2001.

Franco, Celinda. “The MS-13 and 18th Street Gangs: Emerging Transnational Gang Threats?” *CRS Report for Congress*, January 22, 2010. Accessed on August 11, 2010. http://opencrs.com/document/RL34233.

Galbraith, Jay, Diane Downey, and Amy Kates. *Designing Dynamic Organizations*. New York: American Management Association, 2002.

Gates, Robert M. "United States Department of Defense Quadrennial Defense Review Report." U.S. Department of Defense. February 12, 2010. Accessed February 17, 2010. http://www.defense.gov/qdr/images/QDR_as_of_12Feb10_1000.pdf.

Giraldo, Jeanne K., and Harold A. Trinkunas. *Terrorism Financing and State Responses: A Comparative Perspective*. Stanford, CA: Stanford University Press, 2007.

Gilbert, James. "Yuma Border Patrol Agents Arrest MS-13 Gang Member." *Yuma Sun.* Accessed October 13, 2010. http://www.yumasun.com/common/printer/view.php?db=yumasun&id=49993.

Granovetter, Mark. "The Strength of Weak Ties: A Network Theory Revisited." *Social Theory I* (1983): 201–233.

Grdovic, Mark. "SWCS PUB 09-1: A Leader's Handbook to Unconventional Warfare." United States Army John F. Kennedy Special Warfare Center and School. November 2009. Accessed on January 27, 2010. http://www.soc.mil/swcs/swmag/Assets/SWCS%20Publications/Leaders%20Guide%20Final.pdf.

"Groups - Middle East – Active – Lebanon: Hizbullah." *Jane's World Insurgency and Terrorism*, April 29 2010. Accessed on June 4, 2010. http://www4.janes.com.libproxy.nps.edu.

Haaretz News Service, October 29, 2010. Accessed on November 5, 2010. http://www.haaretz.com/news/diplomacy-defense/mexico-thwarts-hezbollah-bid-to-set-up-south-american-network-1.300360.

Hanna, David P. *Designing Organizations for High Performance*. Reading: Addison-Wesley Publishing Company, 1988.

Hannigan, John A. "The Armalite and the Ballot Box: Dilemmas of Strategy and Ideology in the Provisional IRA," *Social Problems*, 33, No. 1 (October 1985): 31–40. JSTOR (800629)

Hanlon, N. "Banking 101 with Chavez and Ahmadinejad" *The Americas Report*, May 07, 2009. Accessed on June 5, 2010. http://www.centerforsecurity.org.

Harness, William J. "MS-13 Mara Salvatrucha." *Conroe ISD Police Department Report* (2006), Accessed on April 11, 2010. http://police.conroeisd.net/Docs/MS%2013%20Gang.pdf.

Henzel, Christopher. "The Origins of al Qaeda's Ideology: Implications for U.S. Strategy." *Parameters*, Spring 2005: 69–79.

“The hijackers... and how they were connected.” *Sydney Morning Herald.* September 22, 2001. Accessed on October 13, 2010.

Horigan, John and Max Taylor, “Playing the Green Card: The Financing of the Provisional IRA, Part 1.” *Terrorism and Political Violence,* 11, No. 2, Summer 1999, 1–20

———. “Playing the Green Card: Financing the Provisional IRA, Part 2,” *Terrorism and Political Violence,* 15, No. 2, Summer 2003, 1–60.

———. “The Provisional Irish Republican Army: Command and Functional Structure”, *Terrorism and Political Violence*, 9: 3, 1997, 1–32. Accessed October 13, 2010. http://dx.doi.org/10.1080/09546559708427413.

Hudson, R. *Terrorist and Organized Crime Groups in the Tri-Border Area (TBA) of South America*. Washington DC: Library of Congress Research Division, 2003.

Hulnick, Arthur S. and Daniel W. Mattasusch. "Ethics and Morality in U.S. Secret Intelligence" in *Ethics of Spying: A Reader for the Intelligence Professional*, edited by Jan Goldman, 520-521. Lanham: Scarecrow Press, 2006.

International Institute for Counter-Terrorism. "ICT Commentaries- Venzuelan Ties to Hezbollah." *International Institute for Counter-Terrorism*. August 18, 2008. Accessed on March 2, 2010. http://www.ict.org.il/NewsCommentaries/Commentaries/.

Jackson, Brian A. “Counterinsurgency Intelligence in a Long War: The British Experience in Northern Ireland,” *Military Review,* (January/February 2002): 74–85.

Jackson, Brian A., John C. Baker, Kim Cragin, John Parachini, Horacio R. Trujillo, Peter Chalk, *Aptitude for Destruction: Case Studies of Organizational Learning in Five Terrorist Groups,* Santa Monica, CA: Rand Corp, 2005.

Jansen, Erik. "MN3121: Organizational Design for Defense Analysis." Naval Postgraduate School, Fall Term 2009.

Jimenez, Edgar A., James S. McCullar, and Kevin M. Trujillo. “Pseudo Operations and Deception in Irregular Conflict.” Naval Postgraduate School, 2010.

Jones, Derek. "Understanding the Form, Function, and Logic of Clandestine Cellular Networks: The First Step in Effective Conternetwork Operations." United States Army Command and General Staff College School of Advanced Military Studies. May 21, 2009. Accessed on November 5, 2009. http://www.cgsc.edu/sams/media/Monographs/JonesD-21MAY09.pdf.

Juergensmeyer, Mark. *Terror in the Mind of God*. Berkeley: University of California, 2003.

Karmon, Eli, *Iran and its Proxy Hezbollah: Strategic Penetration in Latin America Working Paper.* Madrid: Elcano Royal Institute, August 2009. Accessed on October 28, 2010. https://www.realinstitutelcano.org.

Khoury, Jack. "Mexico Thwarts Hezbollah Bid to set up South American Network," June 7, 2010. Accessed December 13, 2010. http://www.haaretz.com/news/diplomacy-defense/mexico-thwarts-hezbollah-bid-to-set-up-south-american-network-1.300360.

Kittner, Cristina Brafman. "The Role of Safe Havins in Islamist Terrorism." *Terrorism and Political Violence* 19, no. 3 (2007): 307–327.

Krackhardt, David. "The Strength of Strong Ties: The importance of Pilios in Organizations." in *Networks and Organizations: Structure, Form, and Action*, by Nitin Nohria and Robert G. Eccles, 216–239. Boston: Harvard Business School Press, 1992.

Krebs, Valdis E. "Mapping Networks of Terrorist Cells." *Connections* 24 (2001): 43–52.

Krul, Chris and Sebastian Rotella, S. "Drug probe finds Hezbollah link; Officials say they've broken up Colombian ring that helped fund the militant group." *Los Angeles Times*, October 22, 2008. Accessed on June 14, 2010. http://www.proquest.com.libproxy.nps.edu/.

Liang, Qiao, and Wang Xiangsui. "Unrestricted Warfare." IWS - The Information Warfare Site. PLA Literature and Arts Publishing House. February 1999. Accessed on October 7, 2009. http://www.iwar.org.uk/iwar/resources/china/iw/unrestricted-warfare.pdf.

LaVerle, Barry, Glenn E. Curtis, Rex A. Hudson, Nina A. Kollars, *A Global Overview of Narcotics Funded Terrorist and Other Extremist Groups*. Washington DC: Library of Congress, 2002. Accessed on June 3, 2010. http://www.loc.gov/rr/frd.

Logan, Sam, Ben Bain and Kate Kairies. “Deportation Feeds a Cycle of Violence in Central America.” *World Press*, March 31, 2006. Accessed on July 11, 2010. http://www.worldpress.org/Americas/2304.cfm.

Looney, Robert E. “Following the Terrorist Informal Money Trail: The Hawala Financial Mechanism. Naval Postgraduate School Center for Contemporary Conflict, Monterey, CA, November 1, 2002.

Martin, Bryan, Gabriel Szody, and Joshua Thiel. “Radical Destabilization: A Low Cost, High Success Policy Option for the United States.” Naval Postgraduate School, 2010.

McCargar, James. "Part 1: Fundementals and Forms of Action." in *A Short Course in the Secret War*, by Christopher Felix, 15–151. Lanham: Madison Books, 2001.

McCormick, G. H., and G. Owen. "Security and Coordination in a Clandestine Organization." *Mathematical and Computer Modeling*, no. 31 (2000): 175–192.

McDermott, Jeremy. “Youths Flock to Massive El Salvadoran Gang that is their Only Chance of a ‘Job’,” *The Scotsman,* sec. International, April 13, 2004. Accessed on April 2, 2010. http://thescotsman.scotsman/international.cfm?id=416482004&format=print.

Milward, H. Brinton, and Joerg Raab. "Dark Networks as Problems Revisited: Adaptation and Transformation of Islamic Terror Organizations since 9/11." University of Southern California. September 29, 2005. Accessed on August 4, 2010. http://www.usc.edu/schools/sppd/private/documents/bedrosian/dark_networks.pdf.

Mintzberg, Henry. *Mintzberg on Management: Inside Our Strange World of Organizations*. New York: The Free Press, 1989.

Mintzberg, Henry. "Organization Design: Fashion or Fit?" *Harvard Business Review* 59, no. 1 (January/February 1981): 103–116.

Miro, Ramon J., “Organized Crime and Terrorist Activity in Mexico, 1999-2002”, *Library of Congress Report* (February 2003), Accessed on November 29, 2010. http://www.loc.gov/rr/frd/pdf-files/OrgCrime_Mexico.pdf.

Miryekta, Cyrus, “Hezbollah in the Tri-Border Area of South America.” *Small Wars Journal*, September 10, 2010. Accessed on October 25, 2010. http://smallwarsjournal.com/blog/journal/docs-temp/533-miryekta.pdf.

Molnar, Andrew R., Jerry M. Tinker, and John D. LeNoir. "Chapter 1: Underground Organization within Insurgency." in *Human Factors Considerations of Undergrounds in Insurgencies*, by Special Operations Research Office, 17–35. Washingtoc D.C.: Special Operations Research Office, 1965.

———. "Chapter 5: Clandestine and Covert Behavior." in *Human Factors Considerations of Undergrounds in Insurgencies*, 101–108. Washington, D.C.: Special Operations Research Office, 1965.

Molnar, Andrew R., William A. Lybrand, Lorna Hahn, James L. Kirkman, and Peter B. Riddleberger. *Undergrounds in Insurgent, Revolutionary, and Resistance Warfare*. Washington, D.C.: Special Operations Research Office, 1963.

Moloney, Ed. *A Secret History of IRA,* 2nd ed., London: Penguin Books, 2007.

Nadler, David, Michael Tushman, and Mark B. Nadler. *Competing by Design: The Power of Organizational Architecture*. New York: Oxford University Press, 1997.

Nagorsky, Thomas. President Ahmedinejad Threatens U.S. With War 'Without Boundaries'. September 21, 2010. Accessed on October 13, 2010. http://abcnews.go.com/International/iran-president-threatens-us-war-boundaries-nuclear-faclities/story?id=11689305&page=1.

National Commission on Terrorist Attacks Upon the United States. “Al Qaeda Aims At The American Homeland.” Accessed on August 30, 2010. http://www.9-11commission.gov/report/911Report_Ch5.htm.

National Counterterrorism Center, “Hizballah,” *Counterterrorism Calendar 2010.* Accessed on November 8, 2010. http://www.nctc.gov/site/groups/hizballah.html.

Obama, Barack. "National Security Strategy." The White House. May 27, 2010. Accessed on May 28, 2010. www.whitehouse.gov/sites/default/files/rss.../national_security_strategy.pdf.

Peters, Gretchen, “Drug Trafficking in the Pacific Has a Distinct Russian Flavor,” *San Francisco Chronicle,* 30 May 2001. Accessed on November 29, 2010. http://articles.sfgate.com/2001-05-30/news/17600134_1_svesda-maru-russians-largest-cocaine-seizure.

Phillippone, Douglas, *Hezbollah: the Network and Its Support Systems, Can They be Stopped?* (Monterey, CA: Naval Postgraduate School, 2008).

“The Plot: A Web of Connections.” *The Washington Post.* September 24, 2001. Accessed October 13, 2010. http://www.washingtonpost.com/wp-srv/nation/graphics/attackinvestigation_24.html.

Prager Security International. *Denial of Sanctuary: Understanding Terrorist Safe Havens*, edited by Michael Innes. Westport: Prager Security International, 2007.

“Provisional Irish Republican Army” *Jane’s World Insurgency and Terrorism*, Jane’s Terrorism and Insurgency Center (2009). Accessed on September 28, 2010. http://www8.janes.com.libproxy.nps.edu/JDIC/JTIC/documentView.do?docId=/content1/janesdata/binder/jwit/jwita107.htm@current&pageSelected=&keyword=&backPath=http://jtic.janes.com/JDIC/JTIC&Prod_Name=JWIT&activeNav=http://www8.janes.com/JDIC/JTIC.

Raab, Jorg, and H. Brinton Milward. "Dark Networks as Problems." *Journal of Public Administration Research and Theory* 13, no. 4 (October 2003): 413–439.

Rabasa, Angel, et al. "Ungoverned Territories: Understanding and Reducing Terrorism Risks." RAND Corporation, 2007. Accessed on October 12, 2009. http://www.rand.org/pubs/monographs/2007/RAND_MG561.pdf.

Robb, John. *Brave New War: The Next Stage of Terrorism and the End of Globalization*. Hoboken, New Jersey: John Wiley & Sons, Inc., 2007.

Roth, John, Douglas Greenburg, and Serena Wille. “Monograph on Terrorist Financing”. National Commission on Terrorist Attacks Upon the United States. Washington, DC: Government Printing Office, August 21, 2004.

Ruppersberger, C.A. “Dutch”. Statement on threat of gangs. Accessed November 6, 2010. http://dutch.house.gov/2006/07/07-14-06-MS13Gang.shtml.

Sageman, Marc. *Leaderless Jihad: Terror Networks in the Twenty-First Century.* Philadelphia: University of Philadelphia Press, 2008.

———. *Understanding Terror Networks.* Philadelphia: University of Philadelphia Press, 2004.

Silke, Andrew, “In Defense of the Realm: Loyalist Terrorism in Ireland Part 1: Extortion and Blackmail*,” Studies in Conflict and Terrorism* (1998): 331–361.

Simons, Anna, and Davis Tucker. "The Misleading Problem of Failed States: A 'Socio-geography' of Terrorism in the Post-9/11 Era." *Third World Quarterly* 28, no. 2 (2007): 387–401.

Sparrow, Malcolm K. "The Application of Network Analysis to Criminal Intelligence: An Assessment of the Prospects." *Social Networks* 13 (1991): 251–274.

Steele, J. Michael. "Models for Managing Secrets." *Management Science* (INFORMS) 35, no. 2 (1989): 240–248.

Stewart, T. “Six degrees of Mohamed Atta.” Business 2.0. December 2001. Accessed October 13, 2010. http://www.business2.com/articles/mag/0,1640,35253,FF.html.

Sullivan, Mark P. *Latin America: Terrorism Issues.* Washington DC: Congressional Research Service, 2009.

Sullivan, John P. and Samuel Logan. “MS-13 Leadership: Networks of Influence.” *The Counter Terrorist.* August/September 2010. Accessed on November 9, 2010. http://digital.ipprintservices.com/display_article.php?id=428186.

“Suspected MS-13 Gang Leader Arrested in Santa Cruz.” KSBW News.com. Accessed December 1, 2010. http://www.ksbw.com/news/23772715/detail.html.

Treverton, G., Matthies, C., Cunningham, K.J., Goulka,J., Ridgeway, G., Wong, *A. Film Piracy,Organized Crime and Terrorism*. Santa Monica, CA: RAND Corporation, 2010.

Turney-High, Harry Holbert. *Primitive War*, 2nd Edition (Columbia: University of South Carolina Press, 1991).

Tzu, Sun. *The Art of War*. Translated by Samuel B. Griffith. London: Oxford University Press, 1971.

United States Congress. “MS-13 and Counting.” *Hearing before the Committee on Government Reform*. House of Representatives, 109th Congress, 2nd Session, July 14, 2006, serial no. 109-174 and September 6, 2006, serial no. 109–182.

United States Congress, *Weak Bilateral Law Enforcement Presence at the U.S.-Mexico Border: Territorial Integrity and Safety Issues for American Citizens*, Joint Hearing of the 109th Congress, 1st Session, November 17, 2005. Washington D.C.: U.S. Government Printing Office, 2006.

United States Department of Justice. "Indictment of ZACARIAS MOUSSAOUI." December 11, 2001. Accessed on November 2, 2010. http://www.usdoj.gov/ag/moussaouiindictment.htm.

United States Department of Justice, "Mara Salvatrucha," *Drugs and Crime Gang Profile*, November 2002. Accessed on November 15, 2010. http://webzoom.freewebs.com/swnmia/mara.pdf.

United States Department of Defense. Transcript of bin Laden Video Tape. December 13, 2001. Accessed on October 13, 2010. http://www.defenselink.mil/news/Dec2001/D20011213ubl.pdf.

United States House of Representatives, Committee on International Relations. *Iran: A Quarter Century of State-Sponsored Terror.* Washington DC: US Government Printing Office, 2005.

United States Senate Committee on Homeland Security and Governmental Affairs. *Hezbollah: Financing Terror Through Criminal Enterprise, Testimony of Dr. Matthew Levitt*. 109th Congress, 1st Sess. May 25, 2005

Van De Ven, Andrew H., Andre L. Delbecq, and Jr., Richard Koenig. "Determinants of Coordination Modes within Organizations." *American Sociological Review* (American Sociological Association) 41, no. 2 (April 1976): 322–338.

Ware, Michael. "Los Zetas called Mexico's most dangerous drug cartel," *CNN.com.* Accessed on November 29, 2010. http://www.cnn.com/209/WORLD/americas/08/06/mexico.drug.cartels/index.html.

White, Robert W. "Don't confuse me with the facts: More on the Irish Republican Army and Sectarianism." *Terrorism and Political Violence* 10, no. 4, (1998): 164–189. Accessed on October 1, 2010. http://dx.doi.org/10.1080/09546559808427487.

White, Robert W. *Provisional Irish Republicans: An Oral and Interpretive History*. Westport, CT: Greenwood Press, 1989.

Wood, Randall, "South America's Tri-Borders Region," *SAIS Review*, 25, No. 1, Winter-Spring 2005, 105.

Woodrow WIlson International Center for Scholars Latin American Program. "Iran in Latin America: Threat or ‘Axis of Annoyance’?" Woodrow Wilson Center Reports on the Americas. 23. Edited by Cynthia Arnson, Haleh Esfandiari and Adam Stubits. Washington, DC, January 2010.

World’s Most Dangerous Gang. DVD. Produced by Andrew Tkach. 2006; U.S.A. and Canada: Warner Home Video, 2006.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia

2. Dudley Knox Library
Naval Postgraduate School
Monterey, California

3. Dr. Nancy Roberts
Department of Defense Analysis
Naval Postgraduate School
Monterey, California

4. Dr. John Arquilla
Department of Defense Analysis
Naval Postgraduate School
Monterey, California

5. Dr. Gordon McCormick
Department of Defense Analysis
Naval Postgraduate School
Monterey, California

6. Jennifer Duncan
Department of Defense Analysis
Naval Postgraduate School
Monterey, California

7. COL Gregory Wilson
Department of Defense Analysis
Naval Postgraduate School
Monterey, California

8. Commander, United States Special Operations Command
ATTN: G3X
MacDill Air Force Base, Florida

9. Commander, United States Army Special Operations Command
ATTN: G3X
Fort Bragg, North Carolina

10. Commander, United States Army Special Forces Command
ATTN: G3X
MacDill Air Force Base, Florida